КИБЕРПРЕСТУПНОСТЬ:
РИСКИ И УГРОЗЫ

Санкт-Петербург
2021

Верховный Суд Российской Федерации

Северо-Западный филиал ФГБОУВО
«Российский государственный университет правосудия»

КИБЕРПРЕСТУПНОСТЬ: РИСКИ И УГРОЗЫ

МАТЕРИАЛЫ
ВСЕРОССИЙСКОГО СТУДЕНЧЕСКОГО
КРУГЛОГО НАУЧНО-ПРАКТИЧЕСКОГО СТОЛА
С МЕЖДУНАРОДНЫМ УЧАСТИЕМ
(11 февраля 2021 г.)

Санкт-Петербург
Астерион
2021

УДК 343.3/.7, 343.97
ББК 67.408
К 38

Сост. и ред.: К. А. Краснова, Е. В. Топильская, Е. А. Васик

К 38 **Киберпреступность: риски и угрозы** : материалы Всероссийского студенческого круглого научно-практического стола с международным участием (Северо-Западный филиал ФГБОУВО «Российский государственный университет правосудия» (Санкт-Петербург, 11 февраля 2021 г.) / Под ред. д-ра юрид. наук, доцента Е. Н. Рахмановой. – Санкт-Петербург : Астерион, 2021. – 236 с.

ISBN 978-5-00188-023-3

В сборник включены доклады выступлений участников Всероссийского научно-практического круглого стола с международным участием «Киберпреступность: риски и угрозы» (СЗФ РГУП, 11 февраля 2021 г.).

Издание может быть рекомендовано преподавателям, научным сотрудникам, аспирантам и студентам юридических вузов, судьям, иным практическим работникам, всем интересующимся уголовно-правовыми и криминологическими проблемами.

УДК 343.3/.7, 343.97
ББК 67.408

ISBN 978-5-00188-023-3

СОДЕРЖАНИЕ

Раздел II

СЕКЦИЯ «ПРОБЛЕМЫ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПНОСТИ»

К. А. Краснова, Е. В. Топильская

ПАНДЕМИЯ НЕ ПРЕГРАДА ДЛЯ СТУДЕНЧЕСКОЙ НАУКИ

Вот уже год, как Северо-Западный филиал РГУП активно использует современные информационные технологии в образовательной и научной деятельности обучающихся. По инициативе заведующей кафедрой уголовного права, доктора юридических наук, доцента *Екатерины Николаевны Рахмановой* 11 февраля 2021 года преподаватели кафедры организовали Всероссийский студенческий круглый научно-практический стол с международным участием в формате видео-конференц-связи на актуальную и наиболее дискуссионную тему последнего времени: «Киберпреступность: риски и угрозы».

В студенческом научном мероприятии приняли участие студенты, магистранты и аспиранты Ташкентского государственного юридического университета (Узбекистан), Донецкого национального университета (Донецкая Народная Республика), филиалов РГУП и ведущих российских вузов – МГЮА, МГИМО МИД России, Московского университета МВД России имени В. Я. Кикотя, Саратовской государственной юридической академии, Самарского национального исследовательского университета имени академика С. П. Королева, Санкт-Петербургского государственного университета, Санкт-Петербургского юридического института (филиала) Университета Прокуратуры Российской Федерации, Санкт-Петербургского института (филиала) ВГУЮ (РПА Минюста), Санкт-Петербургского Политехнического университета Петра Великого, Санкт-Петербургского государственного архитектурно-строительного университета, РГПУ имени А. И. Герцена. В итоге круглый стол собрал более 50 участников с докладами и состоял из Пленарного заседания и заседаний 2-х секций.

С приветственным словом выступили директор Северо-Западного филиала РГУП, доцент кафедры государственно-правовых дисциплин,

председатель суда в отставке, заместитель председателя Санкт-Петербургского отделения Общероссийской общественной организации «Российское объединение судей» *Ярослав Борисович Жолобов* и заместитель директора Северо-Западного филиала РГУП по научной работе, заведующая кафедрой общетеоретических правовых дисциплин, доктор юридических наук, профессор *Александра Андреевна Дорская*.

Открыла работу Пленарного заседания профессор кафедры уголовно-правовых дисциплин Казанского филиала РГУП, доктор юридических наук, доцент *Марина Александровна Ефремова*, которая в рамках своего выступления оценила состояние и основные тенденции киберпреступности в России, озвучила основные показатели преступлений, совершенных с использованием информационно-телекоммуникационных технологий, в 2020 году, с тревогой отметила рост числа кибермошенничеств, в том числе с использованием социальной инженерии. Продолжила работу Пленарного заседания *Кристина Андреевна Иващенко*, аспирант РГУП, которая подчеркнула, что в современной российской экономико-правовой жизни активно обсуждаются вопросы о совершенствовании форм и методов контрольно-надзорной деятельности, пересмотре моделей запрещенных общественно опасных деяний и меры юридической ответственности за совершение новой разновидности киберпреступлений, связанных с созданием цифровых картелей. «Ежедневно появляются новые цифровые инструменты в руках недобросовестных участников рынка, – продолжила К. А. Иващенко, – но некоторые из них уже плотно укоренились в практике антимонопольных органов и требуют отдельного изучения».

Заседание 2-й секции открыл *Манолис Афанасьевич Терсенов* (помощник прокурора г. Тюмени). Он рассказал о трудностях, с которыми сталкиваются сотрудники правоохранительных органов при выявлении, пресечении и расследовании хищений денежных средств с банковских счетов, что в настоящее время является наиболее распространенным видом хищений, а также об особенностях профилактики данного вида преступлений. Участники секции сошлись во мнении, что эффективность противодействия этим преступлениям можно повысить только за счет комплексных мер – разъяснения гражданам правил безопасного поведения в виртуальном пространстве, повышения квалификации и профессионализма сотрудников уголовного розыска и следствия, усиления надзора за раскрытием и расследованием таких преступлений. Кроме того, М. А. Терсенов обратил внимание на важность взаимодействия правоохранительных органов с банковскими учреждениями для

оперативного реагирования на действия злоумышленников и предотвращения причинения материального вреда потерпевшим.

После выступлений экспертов работы круглого стола была продолжена в двух секциях: «Правовая оценка киберпреступности» (модератор – доцент кафедры уголовного права СЗФ РГУП, кандидат юридических наук, доцент *Кристина Александровна Краснова*) и «Проблемы противодействия киберпреступности» (модератор – доцент кафедры уголовного права СЗФ РГУП, кандидат юридических наук *Елена Валентиновна Топильская*).

Участники круглого стола внимательно слушали выступления, задавали вопросы, вели активную дискуссию, высказывали собственное мнение, обменивались опытом. Доклады всех участников были очень интересными, наполненными массой примеров из следственно-судебной практики, и сопровождались яркими презентациями. Все доклады были отмечены сертификатами за участие и включены в настоящий сборник, который размещен в РИНЦ.

Данное мероприятие подтвердило интерес участников к научной жизни и желание контактировать со студентами из других регионов и стран, тем более что современные информационные технологии позволяют это сделать из любого уголка мира. На наших глазах формируется молодое поколение юридического сообщества.

Оргкомитет

Раздел I

СЕКЦИЯ «ПРАВОВАЯ ОЦЕНКА КИБЕРПРЕСТУПНОСТИ»

А. А. Карташов

УГОЛОВНОЕ ПРАВО В ПЕРИОД ЧЕТВЕРТОЙ ПРОМЫШЛЕННОЙ РЕВОЛЮЦИИ

Аннотация: В статье рассматриваются некоторые теоретические, законодательные и практические вопросы, связанные с уголовно-правовой оценкой деятельности систем с искусственным интеллектом.

Ключевые слова: уголовная ответственность, искусственный интеллект, субъект преступления.

CRIMINAL LAW IN THE PERIOD OF THE FOURTH INDUSTRIAL REVOLUTION

Abstract: The article deals with some theoretical, legislative and practical issues related to the criminal legal assessment of the activities of systems with artificial intelligence.

Keywords: criminal liability, artificial intelligence, the subject of the crime.

Наше общество находится на переходной стадии между «информационным строем», начавшимся в середине XX века, и эпохой цифровых технологий, таких как искусственный интеллект (AI), беспилотные автомобили и «Интернет вещей» (IoT) – четвертой промышленной революцией. В складывающихся условиях стремительной цифровизации требуется совершенствование как правовой системы в целом, так и уголовного законодательства в частности.

Прежде чем перейти непосредственно к рассмотрению вопроса модернизации уголовного права в Российской Федерации применительно к искусственному интеллекту, следует дать определение вышеуказанному понятию. Искусственный интеллект – это способность системы интерпретировать определенным образом полученные данные, принимать на их основе оптимальные решения при помощи самообучения (адаптации). Таким образом, система не только действует строго по алгоритму, заложенному в нее создателем, но и может автономно изменять сам алгоритм в определенных границах для оптимизации принятия решений.

Сферы использования систем с искусственным интеллектом разнообразны – от чат-ботов до аналитических систем принятия решений. Не остаются в стороне от использования подобных систем и спецслужбы различных стран. В 2018 году полиция Великобритании запустила прототип National Data Analytics Solution (NDAS). Предполагалось, что данная система на основе машинного обучения и статистики, полученной из базы данных полиции, будет способна предсказать насильственные преступления, которые в будущем способен совершить тот или иной гражданин. Утверждалось, что данная система не будет использоваться для упреждающих арестов, а напротив, она направлена на поспешное оказание медицинской или социальной помощи. Прототип системы, стоивший 10 млн фунтов стерлингов, был готов к 2020 году и получил название Most Serious Violence (MSV). Система работает по принципу баллов риска: чем выше балл, тем больше вероятность, что человек в будущем совершит преступление. Расчет баллов производился с помощью двух критериев: поведенческого – из базы данных полиции бралась информация о возрасте, совершенных преступлениях, количества упоминаний человека в базе и другого; сетевого – система изучала связь человека с лицами, обвинявшимися в совершении тяжких преступлений. Во время тестового запуска выяснилось, что у системы очень низкая точность, около 9–19 %, что и послужило решением об отмене тестирования и дальнейшего запуска[1].

На первый взгляд такое поведение искусственного интеллекта не является критическим. Однако глубокий анализ данной ситуации, связанной с обучением ИИ, указывает на проблемы его «социальной адаптации».

Например, система с ИИ COMPAS (США) указывала на риск повторного совершения преступления, если речь шла об афроамериканце. Возможно, это отражало социально-политические тенденции в обществе, но система могла на основе анализа ответов лица определить его как рецидивиста, даже в том случае, когда он ни разу в жизни не привлекался к уголовной ответственности и не имел конфликтов с законом[2].

Действительно, описанные ситуации произошли при тестовом запуске системы с ИИ, в которых не было пострадавших, но ведь если бы тесты не выявили на начальном этапе этой проблемы, то последствия могли бы быть очень плачевными.

---

[1] Полиция Великобритании два года разрабатывала ИИ-систему прогнозирования преступлений. Но применить ее так и не смогли. URL: https://baza.io/posts/15fb90e7-e1aa-4a2b-b13a-703bff6e1161 (дата обращения: 23.12.2020).

[2] Искусственный интеллект обвинили в расизме // Коммерсантъ. 21.08.2017. URL: https://kommersant.ru/doc/3390196 (дата обращения: 23.10.2020).

В 2018 году Китай начинает активно применять технологии с искусственным интеллектом для распознавания лиц и даже походки с помощью камер слежения. В некоторых городах камеры сканируют железнодорожные вокзалы в поисках самых разыскиваемых преступников. Например, полиция городского округа Чжэнчжоу с помощью очков распознавания лиц на базе ИИ задержала контрабандистов героина на железнодорожном вокзале[1]. Полиция Восточного Китая смогла задержать двадцать пять сбежавших преступников на фестивале[2].

Но в процессе использования было выявлено, что у данной системы есть ряд недостатков, одним из основных является большой процент ложных срабатываний. В отличие от вышеуказанных примеров, систему продолжают активно использовать, что влечет за собой дорогостоящие судебные дела, неправомерные задержания и другие для невиновных граждан.

Элементы искусственного интеллекта присутствуют во многих устройствах и системах: это поисковые системы в Интернете, агрегаторы новостей, навигационные системы, цифровые переводчики. Активно развивается это направление в области финансовых услуг и консалтинга, здравоохранения и транспорта.

Из-за увеличения сферы использования ИИ возникают ситуации, когда такая система становится «участником» общественно-опасных деяний, повлекших тяжкие последствия.

Так, доктор из города Роли, штат Северная Каролина, при управлении автомобилем Tesla включил автопилот, отвлекся от дороги просмотром фильма и на полной скорости протаранил полицейские автомобили, перекрывавшие участок дороги, на котором произошло ДТП. Оба патрульных стояли вблизи своих машин, но по стечению обстоятельств никто не пострадал[3].

Одним из самых резонансных случаев «провала» искусственного интеллекта стал случай наезда беспилотного автомобиля на женщину в штате Аризона (США) в 2018 году, в результате которого она скончалась. Причиной произошедшего была названа сниженная чувствительности

[1] Mozur P. Inside China's Dystopian Dreams: A.I., Shame and Lots of Cameras // The New York Times. 2018. URL: https://nytimes.com/2018/07/08/business/china-surveillance-technology (дата обращения: 23.12.2020).

[2] Jiang S. You Can Run, But Can't Hide From AI in China // CNN. 2018. URL: https://cnn.com/2018/05/23/asia/china-artificial-intelligence-criminals-intl/index (дата обращения: 25.12.2020).

[3] Tesla на автопилоте протаранила две полицейские машины // Lenta.ru. URL: https://lenta.ru/news/2020/08/28/autopilot (дата обращения: 24.12.2020).

у датчиков, отвечающих за сближение с объектами, к этому могла привести налипшая грязь, листва и др. Это не единственный случай дорожно-транспортных происшествий со смертельным исходом с участием систем искусственного интеллекта. Ранее в 2016 и 2018 годах погибли водители автомобилей с включенным автопилотом, не контролировавшие управление[1].

В феврале 2020 года водитель автомобиля Tesla включил автопилот и решил отвлечься на видеоигры, во время движения в автономном режиме автомобиль врезался в бетонный барьер, водитель скончался в больнице[2].

В описанных ситуациях виновными в происшествии признаны водители, несмотря на включенный автопилот, так как головную ответственность за деяние с участием искусственного интеллекта согласно современным нормам уголовного права может нести только человек, который, так или иначе, вступает во взаимодействие с такими системами. В числе таких лиц можно выделить производителя (разработчика) искусственного интеллекта, пользователя такой системы, третьих лиц, которые, не имея соответствующих прав и полномочий по созданию или использованию систем с ИИ, могут влиять на их поведение.

На современном этапе развития искусственный интеллект не обладает свойствами, которые могли бы наделить его правосубъектностью и включить в число возможных субъектов преступления. Говорить об искусственном интеллекте, как о субъекте преступления, можно только после признания у него наличия самосознания.

Но, по нашему мнению, уже сейчас необходимо «модернизировать» уголовное право в РФ, так как легче всего решить проблему на этапе ее формирования.

Список литературы

1. Искусственный интеллект обвинили в расизме // Коммерсантъ. 21.08.2017. URL: https:kommersant.ru/doc/3390196 (дата обращения: 23.10.2020).
2. **Полиция Великобритании два года разрабатывала ИИ-систему прогнозирования преступлений. Но применить ее так и не смогли. URL: https:// baza.io/posts/15fb90e7-e1aa-4a2b-b13a-703bff6e1161 (дата обращения: 23.12.2020).**
3. Tesla на автопилоте протаранила две полицейские машины // Lenta.ru. URL: https://lenta.ru/news/2020/08/28/autopilot (дата обращения: 24.12.2020).

[1] Tesla's Autopilot was involved in another deadly car crash // Wired. URL: https://wired.com/story/tesla-autopilot-self-driving-crash-california (дата обращения: 24.12.2020).

[2] Tesla Autopilot crash driver «was playing video game» // BBC. URL: https://bbc.com/news/technology-51645566 (дата обращения: 25.12.2020).

4. Mozur P. Inside China's Dystopian Dreams: A.I., Shame and Lots of Cameras // The New York Times. 2018. URL: https://nytimes.com/2018/07/08/business/china-surveillance-technology (дата обращения: 23.12.2020).
5. Tesla Autopilot crash driver «was playing video game» // BBC. URL: https:bbc.com/news/technology-51645566 (дата обращения: 25.12.2020).
6. Jiang S. You Can Run, But Can't Hide From AI in China // CNN. 2018. URL: https://cnn.com/2018/05/23/asia/china-artificial-intelligence-criminals-intl/index (дата обращения: 25.12.2020).
7. Tesla's Autopilot was involved in another deadly car crash // Wired. URL: https://wired.com/story/tesla-autopilot-self-driving-crash-california (дата обращения: 24.12.2020).

А. А. Долгополов

ВЛИЯНИЕ ПАНДЕМИИ COVID-19 НА КИБЕРПРЕСТУПНОСТЬ

Аннотация: Автор рассматривает влияние новой коронавирусной инфекции на киберпреступность. В настоящей статье приведен анализ уже имеющихся и потенциальных последствий распространения данной болезни для состояния защищенности информационного общества. Кроме того, автором анализируются трудности, которые могут возникнуть при попытке устранения уже имеющихся проблем для осуществления успешного регулирования такой сферы общественных отношений, как сеть Интернет.

Ключевые слова: киберпреступность, коронавирус, коронавирусная инфекция, компьютерная безопасность.

THE IMPACT OF THE COVID-19 PANDEMIC ON THE CYBERCRIME

Abstract: The author examines the impact of the new coronavirus infection on the cybercrime. In this article you can find an analysis of the existing and potential consequences of the spread of this disease for the protection of the information society. In addition, the author analyzes the difficulties that may arise when mankind will try to eliminate these problems and do they best for successful regulation public relations on the Internet.

Keywords: cybercrime, coronavirus infection, coronavirus, cyberjustice.

Пандемия новой коронавирусной инфекции (COVID-19) внесла значительные изменения в жизнь всего человечества. Прежде всего они связаны с различного рода ограничениями (запрет на проведение массовых мероприятий, соблюдение масочно-перчаточного режима, социальное дистанцирование). Особенно важно упомянуть о введении

обязательного режима самоизоляции для всех граждан России, который был объявлен в марте 2020 года. В связи с тем, что огромному количеству граждан было предписано находиться дома, значительно возросла нагрузка на сеть Интернет, а именно на провайдеров соответствующих интернет-услуг. Вследствие этого на протяжении длительного времени наблюдались множественные перебои в интернет-соединении. Также пользователи Сети жаловались на частые ошибки, которые мешали корректной работе на сайтах государственных структур и ведомств. Кроме того, достаточно сильно активизировались и мошенники, которые стали действовать еще более изощренно, чем до пандемии. А так как, к сожалению, и поставщики интернет-услуг, и обычные пользователи оказались не готовыми к таким глобальным изменениям в их жизни и деятельности, то этим воспользовались злоумышленники[1]. Одной из причин расширения «просторов» для совершения преступлений в сети Интернет можно назвать сокращение сотрудников соответствующих государственных структур, а именно – специалистов, отвечающих за информационную безопасность. В то же время значительное увеличение количества киберпреступлений подтверждают и государственные структуры. В соответствии с официальными данными Министерства внутренних дел Российской Федерации (далее – МВД РФ) об уровне преступности за 2020 год число преступлений, связанных с использованием информационно-коммуникационных технологий, выросло более чем на 94 % по сравнению с соответствующим периодом прошлого года[2].

Общая классификация киберпреступлений, число которых возрастает на фоне распространения коронавирусной инфекции, может быть представлена следующим образом:

- неправомерный доступ к компьютерной информации (срыв дистанционных занятий, осуществление несанкционированного дистанционного управления компьютерами пользователей);
- обман граждан путем создания фишинговых сайтов, «продающих» вакцину, антисептики и иные методы борьбы с коронавирусной инфекцией (посредством данных сайтов преступники обманным путем получают личные данные пользователей, в том числе данных от банковских сервисов);

---

[1] Киберпреступность COVID-19: риски и ответные меры // United Nations Office on Drugs and Crime, 2020. URL: https://мвд.рф/upload/site151/doc/UPN_OON._Doklad_Prestupnost_i_Covid.pdf (дата обращения: 15.01.2021).

[2] См.: Фалалеев М. Айфон вместо отмычки // Российская газета. 2020. 20 авг. № 8239.

- распространение в социальных сетях и при помощи почтовых рассылок специальных ссылок, при переходе по которым на компьютер скачивается программное обеспечение, блокирующее дальнейшую работу устройства;
- продажа посредством использования незаконных сетей DarkNet персональных данных граждан, а также иной охраняемой законом информации, которая получена противоправным путем. Кроме того, на подобных площадках антисоциальные элементы обмениваются способами по осуществлению своей недопустимой деятельности, а также распространяют противозаконные вещи, в том числе наркотические вещества;
- распространение заведомо ложной информации об эпидемии COVID-19 и мерах, принимаемых государством в сложившейся ситуации, что является наказуемым в соответствии с действующим законодательством;
- осуществление кибератак на сайты органов государственной власти, учреждений здравоохранения, социальных служб с целью неправомерного доступа к информации, нарушения порядка их работы, а также с целью вымогательства;
- вымогательство посредством направления гражданам сообщений в социальных сетях или на адреса электронной почты (зачастую о том, что последние замечены в совершении преступных действий, или же с просьбой о перечислении денег на благотворительные мероприятия). Как правило, в подобных обращениях преступники просят перевести денежные средства на счет в криптовалюте Bitcoin, так как перемещения денежных масс в данной системе практически невозможно отследить.

Однако недопустимо считать, что правоохранительные органы и представители государственных структур не принимают никаких мер. Напротив, они очень оперативно реагируют на любые правонарушения в сфере, связанной с информационно-коммуникационными сервисами[1]. Более того, еще задолго до этого с целью реализации мер превентивного характера Российская Федерация в ходе 74-й сессии Организации Объединенных Наций предложила под эгидой ООН согласовать и утвердить конвенцию по борьбе с преступлениями в сфере использования информационно-коммуникационных

[1] См.: Козлова Н. Найти шутника // Российская газета. 2020. 22 апр. № 8143.

технологий[1], которая бы позволила осуществлять эффективное международное сотрудничество в сфере борьбы с киберпреступностью.

Анализируя данную ситуацию, можно сделать вывод о том, что помимо усиления правового регулирования, основным методом борьбы с киберпреступностью является повышение правовой культуры населения, в том числе просвещение граждан в сфере компьютерной грамотности. Дело в том, что одним из наиболее часто совершаемых преступлений в Интернете является вымогательство, включая персональные данные. А в случае, если граждане будут предупреждены об опасности предоставления своих данных и иных действиях, посредством которых мошенники могут обмануть их, то количество преступлений соответствующей категории будет существенно снижаться.

К сожалению, при всем многообразии правовых инструментов, имеющихся в наличии у органов государственной власти, на данный момент еще наблюдаются некоторые сложности в их применении для борьбы с деятельностью преступных элементов в информационно-телекоммуникационной сети Интернет. В то же время руководство уполномоченных органов государственной власти, надо признать, предпринимает немало усилий по оптимизации организационной структуры и повышению эффективности своей работы, что является необходимым условием для систематической и результативной деятельности по предупреждению и пресечению киберпреступности. В ключе этих рассуждений невозможно не упомянуть об инициированной Председателем Правительства Михаилом Мишустиным реформы государственного аппарата. В рамках ее осуществления будет оптимизирован штат государственных гражданских служащих в центральных и территориальных органах государственной власти, что, как отмечает Руководитель Аппарата Правительства Дмитрий Григоренко, позволит системе государственного управления стать «более четкой, логичной, отвечающей требованиям времени»[2].

Однако государству не следует останавливаться на достигнутом: злоумышленники продумывают все более изощренные способы мошенничества в Сети, и поэтому необходимо действовать на опережение, принимать превентивные (профилактические) меры с целью расширения возможностей

[1] Противодействие использованию информационно-коммуникационных технологий в преступных целях // United Nations Office on Drugs and Crime, 2019. URL: https://www.unodc.org/documents/Cybercrime/SG_report/V1908184_R.pdf (дата обращения: 16.01.2021).

[2] Правительство утвердило дополнительные параметры реформы госаппарата / Правительство России, 2021. URL: http://government.ru/news/41299/ (дата обращения: 17.01.2021).

государства в борьбе с преступностью в информационно-телекоммуникационных сетях. В связи с этим в рамках осуществления государственной политики сегодня как никогда актуальной является задача совершенствования правового и организационного механизма функционирования соответствующих органов государственной власти. И будет достаточно несправедливо не сказать о том, что еще нет определенных успехов в этом направлении государственной политики. На официальные сайты многих государственных структур уже установлены дополнительные сервисы для их защиты от кибератак и иных видов преступных посягательств. Кроме того, органами государственной власти осуществляется повышение правовой и компьютерной грамотности граждан посредством проведения просветительских мероприятий (в частности, в связи с действием ограничительных мер – преимущественно в дистанционном формате), размещения информационных материалов на официальных интернет-площадках соответствующих ведомств. Помимо этого, на официальном сайте Министерства внутренних дел Российской Федерации имеется возможность подать обращение в специализированное управление «К» (данное управление занимается борьбой с преступлениями, которые связаны с использованием информационно-коммуникационных технологий), что является дополнительной возможностью для граждан помочь в борьбе с преступностью в данной сфере, своевременно сообщив о правонарушении.

Список литературы

1. Киберпреступность COVID-19: риски и ответные меры // United Nations Office on Drugs and Crime, 2020. URL: https://мвд.рф/upload/site151/doc/UPN_OON._Doklad_Prestupnost_i_Covid.pdf (дата обращения: 15.01.2021).
2. Козлова Н. Найти шутника // Российская газета. 2020. 22 апр. № 8143.
3. Правительство утвердило дополнительные параметры реформы госаппарата / Правительство России, 2021. URL: http://government.ru/news/41299/ (дата обращения: 17.01.2021).
4. Противодействие использованию информационно-коммуникационных технологий в преступных целях // United Nations Office on Drugs and Crime, 2019. URL: https://www.unodc.org/documents/Cybercrime/SG_report/V1908184_R.pdf (дата обращения: 16.01.2021).
5. Ульянов М. В. Противодействие преступности в сфере информационно-коммуникационных технологий в условиях применения карантинных мер // Национальная безопасность. 2020. № 2.
6. Фалалеев М. Айфон вместо отмычки // Российская газета. 2020. 20 авг. № 8239.
7. Черноусов И. Эксперты назвали тенденции киберпреступлений в период пандемии // Российская газета, 2020. URL: https://rg.ru/2020/10/23/eksperty-nazvali-tendencii-kiberprestuplenij-v-period-pandemii.html (дата обращения: 16.01.2021).

Я. О. Лапшова

ПРОБЛЕМА УГОЛОВНО-ПРАВОВОЙ ОЦЕНКИ КИБЕРПРЕСТУПНОСТИ

Аннотация: В данной работе рассматривается понятие «киберпреступность». Цель данного исследования – теоретический анализ проблем уголовно-правовой оценки киберпреступности. Автор подчеркивает необходимость унифицированной классификации киберпреступности. При проведении исследования использовался комплексный анализ, включающий в себя историко-правовой, формально-логический и сравнительно-правовой методы. Полученные результаты позволили выделить основные проблемы предотвращения киберпреступлений.

Ключевые слова: киберпреступность, киберпреступления, виртуальное пространство, информационные технологии.

THE PROBLEM OF CRIMINAL LAW ASSESSMENT OF CYBERCRIME

Abstract: The object of this paper is the concept of "cybercrime". The aim is a theoretical analysis of the problems of criminal and legal assessment of cybercrime. We emphasize the need for a unified classification of cybercrime. The research methods area comprehensive analysis, historical-legal, formal-logical and comparative-legal methods. Theoretical result is the following: the main problems of preventing cybercrime were identified.

Keywords: cybercrime, cybercrime, virtual space, information technologies.

В современных условиях пандемия коронавирусной инфекции привела к тому, что применение виртуального пространства резко расширилось. Переход бизнес-структур, образовательных услуг, банковского сектора, потребительского рынка и т. д. в интернет-пространство привел к росту киберпреступности. Следовательно, уголовно-правовая оценка киберпреступности в рамках современного информационного общества становится актуальной проблемой на сегодняшний день. Криминальные слои населения 90-х годов на современном этапе уходят на второй план, довольствуясь ранее полученным заработком. С появлением сети Интернет, компьютеризацией общества появляется большое количество «молодых» преступников, мышление которых кардинально отличается от преступников, ушедших на второй план.

На современном этапе Уголовный кодекс РФ не содержит четкого определения «киберпреступность», но в связи с популяризацией совершения данных преступлений, сложился комплекс нелегальных понятий, таких как компьютерные преступления, преступление в сфере высоких технологий и другие.

Следователи и дознаватели выделяют ряд преступлений, закрепленных Уголовным кодексом РФ, которые чаще всего встречаются при совершении киберпреступлений: «мошенничество в сфере компьютерной информации», «создание, использование вредоносных компьютерных программ», «кража», «незаконное получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну» и др.[1] Недостаточность законодательства, регулирующего борьбу с преступлениями в Интернете, отвечающего современным потребностям правоприменения, не позволяет объективно оценивать масштабы киберпреступности, связанной с новыми коммуникационными технологиями.

Ученые-практики выделяют ряд особенностей киберпреступлений, которые позволяют их классифицировать по таким основаниям, как средства, способ, цель, объекты и субъекты[2]. Средствами таких преступлений являются компьютерная техника, мобильные телефоны и иные информационные носители. Киберпреступления совершаются в особом виртуальном пространстве, что позволяет лицам, совершающих преступления, находиться в разных городах или даже государствах с лицом или лицами, на которых направлено общественно-опасное деяние. Киберпреступления могут иметь одномоментный или продолжительный характер, кибератаки, распространения спама могут продолжаться от нескольких мгновений до нескольких лет, что затрудняет раскрытие таких преступлений[3].

Выделение киберпреступности в отдельный вид преступлений на данный момент определяет лишь конкретные виды и способы совершения такого преступления, что дает возможность преступникам изменять методы деяния, позволяя уйти от ответственности. С каждым годом информационные технологии получают все большее распространение среди населения. Сетевая система не статична, она находится на этапе постоянного развития, изменяясь каждый день, тем самым затрудняя процесс законодательного закрепления всех способов совершения киберпреступлений и установления органами государственной власти базы для раскрытия таких преступлений.

---

[1] См.: Жуков А. З. Киберпреступность: актуальные проблемы и уголовно-правовая оценка в системе современного права // Проблемы экономики и юридической практики. 2019. Т. 15. № 4. С. 141–143.

[2] См.: Куява Т. Ю. Киберпреступность: проблемы уголовно-правовой оценки и организации противодействия // Молодой ученый. 2016. № 29 (133). С. 255–257.

[3] См.: Коробеев А. И., Дремлюга Р. И., Кучина Я. О. Киберпреступность в Российской Федерации: криминологический и уголовно-правовой анализ ситуации // Всероссийский криминологический журнал. 2019. Т. 13. № 3. С. 416–425.

Помимо слабой законодательной основы противодействия киберпреступности одной из основных проблем является недостаточность компетентных лиц, выявляющих и предотвращающих киберпреступления[1]. Трудности возникают с момента проведения осмотра места происшествия или назначения судебной экспертизы, что является рядовой процедурой каждого следователя при совершении преступлений вне киберпространства. Определение места происшествия невозможно без установления обстановки, при которой было совершено преступление. Специалистам не хватает знаний и навыков для определения данной обстановки в киберпространстве.

Лица, преступления которых не связаны с сетью Интернет, по данным портала правовой статистики Генеральной Прокуратуры Российской Федерации, составляют 28 % – среди женщин и 20 % – среди мужчин, не имевших высшего полного образования[2]. Киберпреступники для полноценного завершения преступления должны обладать достаточными научными знаниями в различных областях. Зачастую осведомленность преступников в Интернете превышает осведомленность сотрудников правоохранительных органов.

Таким образом, проблема уголовно-правовой оценки киберпреступности вытекает из слабой законодательной основы, сложности сбора доказательств и самого процесса доказывания, недостатка компетентных лиц в области информационных технологий в органах государственной власти, отсутствия обобщенной судебной системы и иных факторов, влияющих на развитие противодействия киберпреступности.

Список литературы

1. Жуков А. З. Киберпреступность: актуальные проблемы и уголовно-правовая оценка в системе современного права // Проблемы экономики и юридической практики. 2019. Т. 15. № 4. С. 141–143.
2. Коробеев А. И., Дремлюга Р. И., Кучина Я. О. Киберпреступность в Российской Федерации: криминологический и уголовно-правовой анализ ситуации // Всероссийский криминологический журнал. 2019. Т. 13. № 3. С. 416–425.
3. Куява Т. Ю. Киберпреступность: проблемы уголовно-правовой оценки и организации противодействия // Молодой ученый. 2016. № 29 (133). С. 255–257.

[1] См.: Лясковец А. В., Захарова С. В., Лясковец Т. Л. Современная киберпреступность: проблемы уголовно-правовой оценки и организации противодействия // Сборник научных трудов Международной научно-практической конференции, в 2 т. М., 2015. С. 216–219.

[2] Генеральная прокуратура РФ. Портал правовой статистики. URL: https://crimestat.ru/social_portrait (дата обращения: 10.02.2021).

4. Лясковец А. В., Захарова С. В., Лясковец Т. Л. Современная киберпреступность: проблемы уголовно-правовой оценки и организации противодействия // Сборник научных трудов Международной научно-практической конференции, в 2 т. М., 2015. С. 216–219.

М. З. Исмоилова

НЕКОТОРЫЕ УГОЛОВНО-ПРАВОВЫЕ АСПЕКТЫ БОРЬБЫ С КИБЕРПРЕСТУПНОСТЬЮ В РЕСПУБЛИКЕ УЗБЕКИСТАН

Аннотация: В статье рассматривается киберпреступность как реальная угроза безопасности современного общества, анализируются особенности преступлений, совершаемых в киберпространстве. Исследуются меры защиты, принимаемые в Республике Узбекистан с целью прекращения всех аспектов киберпреступности. Определяются опасные общепризнанные международным сообществом виды кибермошенничества и пути защиты от него. В заключение делается вывод о том, что для борьбы с киберпреступностью необходимы новые подходы с использованием достижений науки и техники, а также подготовка сотрудников предприятий и учреждений, в совершенстве отвечающих требованиям современности.

Ключевые слова: киберпреступность, кибермошенничество, компьютерная сеть, киберпространство, хакер.

SOME CRIMINAL ASPECTS OF COMBATING CYBERCRIME IN THE REPUBLIC UZBEKISTAN

Abstract: The article examines cybercrime as a real threat to the security of modern society, analyzes the features of crimes committed in cyberspace. What protection measures are being taken in the Republic of Uzbekistan in order to end all aspects of cybercrime. Dangerous types of cyber fraud, generally recognized by the international community, and ways of protection against it are determined. In conclusion, it should be concluded that the fight against cybercrime requires new approaches using the achievements of science and technology, as well as training employees of enterprises and institutions to perfection, meeting the requirements of the present.

Keywords: cybercrime, cyber fraud, computer network, cyberspace, hacker.

«Более 53 % населения Земли, или 4,1 млрд человек, имеют доступ к Интернету, и это число продолжает расти» – говорится в опубликованном в Женеве докладе Международного союза электросвязи (МСЭ) «Измерение цифрового развития: факты и цифры за 2019 год». На сегодняшний день большинство своего времени люди проводят в Интернете

с целью занятия бизнесом, выполнения служебных обязанностей, проведения финансовой операции, но и для приобретения новых знакомств, общения и развлечения. Это является подтверждением того, что любой человек имеет доступ к компьютерным «всевозможностям». В результате этого некоторые стали использовать интернет-пространство для своей противоправной деятельности.

Киберпреступность – это преступность в информационном пространстве, целью которой является неправомерное использование компьютера, компьютерной сети или сетевого устройства. Киберпреступления представляют реальную угрозу экономической и правовой безопасности современного общества.

Большинство из киберпреступлений совершается киберпреступниками или хакерами, которые зарабатывают на этом деньги. Киберпреступная деятельность осуществляется отдельными лицами или организационными группами. Некоторые киберпреступники объединяются в организованные группы, используют передовые методы и обладают высокой технической квалификацией, а другие – начинающие хакеры, совершавшие информационные преступления в свою пользу.

В сущности, киберпреступники редко совершаются по причинам, не имеющим отношения к получению прибыли, в большинстве случаев они исходят из политических или личных интересов. Среди киберпреступлений широко распространялись две категории: в первом случае, преступники используют вирусы и другие типы вредоносных программ, чтобы заразить компьютеры и таким образом повредить их или остановить их работу. Во втором – киберпреступления используют компьютеры или сети для распространения вредоносных программ, нелегальной информации или неразрешенных изображений. Однако Министерство юстиции США считает, что есть и третья категория киберпреступлений, когда компьютер используется как соучастник незаконного деяния, например, для хранения на нем украденных данных.

Компьютер, зараженный вредоносной программой, может использоваться злоумышленниками для достижения разных целей. К ним относятся кража конфиденциальных данных, политической тайной информации, использование компьютера для совершения других преступных действий или нанесение ущерба данным.

По темпам роста такого рода преступление опережает все остальные виды преступлений. В 2012 году компания Symantec представила доклад «2012 Norton Cybercrime Report», в котором опубликовала результаты исследования по статистике киберпреступлений и оценила

общий ущерб пользователей в 110 млрд[1]. Одно из самых известных преступлений было в мае 2017 года, когда хакерами был запущен вирус-вымогатель WannaCry, который шифровал компьютерные файлы и требовал выкуп за дешифровку. Этот вирус атаковал устройства более чем в 150 странах мира. Следовательно, жертвами киберпреступников могут стать не только отдельные люди, но и целые государства. В апреле 2007 года мощная кибератака в Эстонии парализовала работу всех государственных структур. В Иране в 2010 году специально разработанный вирус Stuxnet вывел из строя центрифуги для обогащения урана, замедлив иранскую ядерную программу на несколько лет.

В Республике Узбекистан, благодаря последовательной и взвешенной политике руководства страны, начали широко внедрять информационно-коммуникационные технологии. Все больше коммерческие и некоммерческие организации Узбекистан создают собственные вебсайты и автоматизированные базы данных, растут масштабы компьютеризации, внедряются современные мобильные и сетевые технологии. Кроме того, в последние годы Республика Узбекистан активно осуществляет интеграцию в международное сообщество. Это посодействовало принятию ряда нормативно-правовых актов в законодательной системе Узбекистана, в соответствии с которыми стали развиваться и совершенствоваться информационно-коммуникационная сфера, регламентироваться отношения между субъектами этого рынка. В них предусматриваются и вопросы обеспечения информационной безопасности.

Например, Уголовный кодекс был дополнен главой 20 «Преступления в сфере информационных технологий» согласно Закону Республики Узбекистан от 25 декабря 2007 года № ЗРУ-137 «О внесении изменений и дополнений в некоторые законодательные акты Республики Узбекистан в связи с усилением ответственности за совершение незаконных действий в области информатизации и передачи данных»[2]. В ней закреплены меры наказания за нарушение правил информатизации, незаконный (несанкционированный) доступ к компьютерной информации,

[1] См.: Зверева Е. Б. Киберпреступность как угроза безопасности современного общества: виды, особенности, методы борьбы и профилактики // Молодой ученый. 2020. № 10 (300). С. 35–37.

[2] Закон Республики Узбекистан от 25 декабря 2007 года № ЗРУ-137 «О внесении изменений и дополнений в некоторые законодательные акты Республики Узбекистан в связи с усилением ответственности за совершение незаконных действий в области информатизации и передачи данных» // Национальная база данных законодательства республики Узбекистан. URL: https://lex.uz/ru/docs/1295264 (дата обращения: 10.02.2021).

компьютерный саботаж, создание и использование или распространение вредоносных программ.

В 2016 году между Министерством по развитию информационных технологий и коммуникаций Республики Узбекистан и правоохранительными органами страны был подписан и введен в действие Регламент по части анализа, идентификации нарушителей, методов и средств, используемых при проведении несанкционированных либо деструктивных действий в информационном пространстве. Это позволило сформировать эффективный механизм взаимодействия между Министерством и правоохранительными органами страны.

В целях усиления борьбы с киберпреступностью при Генеральной прокуратуре Республики Узбекистан был создан новый департамент. Одной из его задач является повышение профессионального уровня сотрудников правоохранительных органов при проведении расследований преступлений, связанных с использованием современных информационно-коммуникационных технологий.

Борьба против киберпреступности стала не только личным делом отдельных государств, но и ряда международных организаций, которые с целью защиты от посягательства киберпреступников акцентируют больше внимания на разработке эффективных международно-нормативных документов как фундаментальной основы при разработке государствами-участниками своего законодательства. Одним из таких международных актов является Конвенция о преступности в сфере компьютерной информации ETS № 185 (Будапешт, 23 ноября 2001 год). Она была принята с целью защиты мирового сообщества от кибермошенничества. В ней названы следующие виды деятельности с использованием компьютеров, которые считаются киберпреступлениями: незаконный перехват или кража данных; компрометация компьютерных систем и сетей; нарушение авторских прав; незаконные азартные игры; продажа запрещенных предметов в Интернете; домогательство, производство или хранение детской порнографии.

Если говорить о способах защиты от последствий кибермошенничества, то существует несколько методов защиты компьютеров от информационных преступлений и атак, соблюдение которых не допускает возникновения и проникновения заразных вирусов в компьютерные сети:

1. Постоянное обновление программного обеспечения и операционной системы, которое гарантирует, что для защиты компьютера используются новейшие исправления безопасности.
2. Использование антивируса или комплексного решения для обеспечения интернет-безопасности.

3. Использование сильных паролей, которые трудно подобрать. Также рекомендуется нигде их не записывать. Можно воспользоваться услугой надежного менеджера паролей, который облегчит задачу, предложив сгенерированный им сильный пароль.
4. Классический способ заражения компьютеров с помощью вредоносных атак и других типов киберпреступлений – это вложения в электронных спам-сообщениях. Не следует открывать вложение от неизвестного отправителя.
5. Вредоносные ссылки в спамовых электронных письмах, а также на незнакомых веб-сайтах. Не следует переходить по этим ссылкам, чтобы не стать жертвой интернет-мошенников.
6. Не передавать личные данные по телефону или по электронной почте, если нет уверенности, что телефонное соединение или электронная почта защищены.

Исходя из вышеизложенного, можно сделать вывод о том, что киберпреступность представляет собой реальную угрозу безопасности и мира современного общества и человечества, отнимает доверие не только к людям, но и к компетенциям государственной власти и международных организаций. Поэтому, помимо указанных наверху подходов и решений, для борьбы с киберпреступностью необходимы еще свежие подходы, основанные на широком использовании успехов науки и техники, а также подготовка сотрудников нового поколения, в совершенстве владеющих навыками компьютерных технологий и компьютерного программирования.

Список литературы

1. Авчаров И. В. Борьба с киберпреступностью // Информатизация и информационная безопасность правоохранительных органов. Материалы XI межд. конф. М., 2012. С. 191–194.
2. Зверева Е. Б. Киберпреступность как угроза безопасности современного общества: виды, особенности, методы борьбы и профилактики // Молодой ученый. 2020. № 10 (300). С. 35–37.

М. Г. Терехов

О РОЛИ ФОРМИРОВАНИЯ ЦИФРОВОГО ПРАВА В СИСТЕМЕ РОССИЙСКОГО ЗАКОНОДАТЕЛЬСТВА КАК ФАКТОРА ПРЕДУПРЕЖДЕНИЯ ПРЕСТУПНОСТИ

Аннотация: В XXI веке состояние системы права России ориентировано на трансформацию правовых отношений в условиях продолжающейся цифровизации общества. Сфера цифровых правоотношений, складывающаяся в сети Интернет, достаточно свободна от правового регулирования национального законодательства и является благоприятной средой для киберпреступности. Научное и законодательное определение единой структуры цифровых правоотношений позволит государству систематизировано контролировать возникающие тенденции цифровых технологий. Для реализации процессов по созданию единой структуры цифровых правоотношений вполне обоснованным является выделение цифровых правоотношений в единую отрасль права с характерным признаком множества межотраслевых институтов – цифровое право.

Ключевые слова: цифровые правоотношения, цифровое право, цифровая экономика, киберпреступность.

ON THE ROLE OF DIGITAL LAW FORMATION IN THE SYSTEM OF RUSSIAN LEGISLATION AS A FACTOR OF CRIME PREVENTION

Abstract: In the first half of the XXI century, the state of the Russian legal system in the context of the digitalization of public relations, of course, is focused on the transformation of legal relations. The sphere of digital legal relations, which is developing in the Internet, is quite free from the legal regulation of national legislation and is a favorable environment for cybercrime. Scientific and legislative definition of a single structure of digital legal relations will allow the state to systematically monitor emerging trends in digital technologies. To implement the processes of creating a unified structure of digital legal relations, it is quite reasonable to separate digital legal relations into a single branch of law with a characteristic feature of many intersectoral institutions-digital law.

Keywords: digital legal relations, digital law, digital economy, cybercrime.

Для всего мирового сообщества 2020 год стал достаточно нестабильным во всех сферах жизни, приход пандемии сильно отразил действительную значимость IT-технологий, цифровых правоотношений в повседневной жизни граждан, сфере бизнеса, государственном управлении. Большинство граждан перешли на дистанционный формат обучения, работы, осуществления гражданско-правовых действий,

связанных с оборотом имущества, в том числе с помощью сети Интернет[1].

По данным МВД России, в 2020 году число преступлений, совершенных с использованием информационно-телекоммуникационных технологий, возросло на 73,4 %, в том числе с использованием сети Интернет – на 91,3 %, при помощи средств мобильной связи – на 88,3 %[2].

Данный факт, безусловно, является беспрецедентным с точки зрения защищенности граждан от IT-угроз в сфере цифровых правоотношений, что ориентирует автора данной научной статьи провести дальнейший анализ складывающихся проблем в сфере цифровых правоотношений, тем самым определить возможные механизмы разрешения достаточно сложной складывающейся оперативной обстановки.

Большое внимание в приоритетном порядке правоохранительными органами уделяется в последнее время профилактике и предупреждению преступлений, совершенных при использовании информационно-телекоммуникационных технологий, где наиболее распространенными деяниями являются кражи, мошенничество.

Такого рода преступления ориентированы на списание денежных средств со счетов банковских карт граждан и личное преступное обогащение злоумышленников, что в целом обуславливает проблематику, которая складывается вокруг массовости совершения подобных противоправных деяний за последнее время (период 2019–2020 годы).

В настоящее время определены причины и условия увеличения количества подобных преступлений, они связаны с массовым уходом граждан в дистанционную среду коммуникации. Данные процессы побуждают граждан наиболее часто пользоваться сервисами сети Интернет, а как следствие, появляются возможности совершения противоправных действий в отношении пользователей сервисами сети Интернет. Постепенно в рамках снижения уровня зараженности в период пандемии снижается и количество преступлений, совершенных с использованием информационно-телекоммуникационных технологий.

Анализ официальных статистических данных, которые приводятся МВД России, указывает на осложненный характер оперативной обстановки в сфере цифровых правоотношений.

---

[1] См.: Волкова М. А., Ленковская Р. Р., Кулешов Г. Н., Незнамова А. А., Туркин М. М., Жестеров П. В., Савцова Н. А. Гражданско-правовое регулирование охраны и защиты авторских прав в сети Интернет. М., 2019.

[2] Краткая характеристика состояния преступности в Российской Федерации за январь–декабрь 2020 года. URL: https://xn--b1aew.xn--p1ai/reports/item/22678184/ (дата обращения: 20.01.2021).

Тенденции данного вида преступлений указывают на устойчивый рост преступности различного характера в данной среде, а также достаточно большой объем латентных преступлений, которые по тем или иным причинам остаются не учтенными в официальной статистике МВД России за отчетные периоды времени.

Основной и наиболее распространенной чертой (признаком) совершения подобных преступлений в Интернете является оборот цифровых активов. Под цифровыми активами подразумевается, что это, в той или иной мере, ценный цифровой объект, выступающий имуществом пользователя (держателя цифрового актива) с характерными свойствами, примером может послужить криптовалюта[1].

По мнению автора, затрудненность правоохранительных органов в раскрытии преступлений, совершаемых с использованием сети Интернет, затрудняется отсутствием познаний в сфере цифровых правоотношений. Достаточно сильно размыты понятия о том, что это такое и как в сфере цифровых правоотношений осуществляются гражданско-правовые и иные юридически значимые действия, еще и в силу отсутствия конкретного законодательства, которое регулирует данные процессы.

В настоящее время наиболее общими правовыми основаниями в рамках гражданско-правовых действий является ст. 141.1 ГК РФ («Цифровые права»), которая достаточно неопределенно разграничивает правовое поле действия цифровых правоотношений, а также сущность режима цифровых правоотношений.

За последнее время, безусловно, наиболее важным и приоритетным направлением для науки и законодательства является структурированное формирование понятия о цифровых правоотношениях, что вполне обоснованно указывает на предпосылки формирования в юриспруденции новой отрасли права – цифрового права, которое рассматривается на сегодняшний день через существование полноценного межотраслевого института цифровых активов[2].

Подводя итог, следует отметить, что при систематизированном научном подходе к проблеме цифровизации общества, а также благодаря достаточно обширному пониманию складывающейся проблемы

---

[1] См.: Тумаков А. В., Терехов М. Г. Создание финансовых пирамид с использованием цифровых активов // Вестник экономической безопасности. 2020. № 3. С. 92.

[2] Федеральный закон от 31.07.2020 № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» // СПС «Консультант Плюс», 2021.

сотрудниками правоохранительных органов станет возможным осуществлять раскрытие преступлений, связанных с использованием цифровых активов, на основе сформированных структурных эмпирических знаний о таком феномене, как цифровые правоотношения.

Список литературы

1. Волкова М. А., Ленковская Р. Р., Кулешов Г. Н., Незнамова А. А., Туркин М. М., Жестеров П. В., Савцова Н. А. Гражданско-правовое регулирование охраны и защиты авторских прав в сети Интернет. М., 2019.
2. Тумаков А. В., Терехов М. Г. Создание финансовых пирамид с использованием цифровых активов // Вестник экономической безопасности. 2020. № 3. С. 91–94.

К. С. Павкова

ЭЛЕКТРОННЫЕ СРЕДСТВА ПЛАТЕЖА КАК ПРЕДМЕТ ПРЕСТУПЛЕНИЙ ПРОТИВ СОБСТВЕННОСТИ

Аннотация: В статье рассматривается новый подход к трактовке понятия предмета преступлений против собственности, исследуется правовой статус «электронных» средств платежей, в том числе криптовалют в России. Затронуты гражданско-правовые и уголовно-правовые аспекты этого явления. Отмечается, что законодательство умалчивает о правовом статусе криптовалют, а теория и судебная практика не выработали единого подхода.

Ключевые слова: предмет преступления, хищение, криптовалюта.

ELECTRONIC MEANS OF PAYMENT AS A SUBJECT OF CRIMES AGAINST PROPERTY

Abstract: The article considers a new approach to the interpretation of the concept of the subject of crimes against property, examines the legal status of “electronic” ways of payment, including cryptocurrencies, in Russia. The civil and criminal aspects of this phenomenon are touched upon. It is noted that the legislation is silent about the legal status of cryptocurrencies, and theory and judicial practice have not developed a single approach.

Keywords: subject of crime, theft, cryptocurrency.

Цифровизация вкупе с удешевлением средств автоматизированной обработки (передачи) данных и экспонентным ростом числа пользователей современными технологиями предоставила криминальному миру новые возможности, что вызвало рост числа совершаемых преступлений. Ответом стала законодательная дифференциация уголовной ответственности за так называемые киберпреступления, что позволило уточнить предметы новых видов хищений.

Совершение киберпреступлений одновременно в двух мирах – экономическом и информационно-технологическом определяет их социально-правовую сущность. Для указанных составов преступлений обязательным признаком выступает наличие предмета[1], которым могут быть, согласно ГК РФ, имущество и вещно-правового характера, и «бестелесное», в том числе имущественные права, включая безналичные денежные средства, бездокументарные ценные бумаги, цифровые права. В этой связи возникает вопрос о возможности признания предметом компьютерных хищений электронных денежных средств и криптовалюты.

Основным отличием между электронными и безналичными денежными средствами является наличие (у безналичных) либо отсутствие (у электронных) банковского счета, на который зачисляются и с которого переводятся денежные средства, что не имеет принципиального значения для уголовного права, что подчеркивается в п. 5 Постановления Пленума Верховного Суда РФ от 30 ноября 2017 года № 48, в п. 1 Постановления Пленума Верховного Суда РФ от 7 июля 2015 года № 32. Также на практике суды относят безналичные и электронные денежные средства к имуществу, а не к праву на имущество, в связи с этим практика относит их к предметам хищения, а не к мошенничеству в форме приобретения права на имущество (нашло отражение в Постановлении Пленума Верховного Суда РФ от 30 ноября 2017 года № 48). Таким образом, Верховный суд фактически отверг содержащийся в учении о хищении физический признак имущества[2]. Вышеуказанный подход способствует более эффективному применению норм об ответственности за хищения[3].

В соответствии с ч. 2 ст. 1 Федерального закона № 259-ФЗ цифровыми финансовыми активами признаются «цифровые права, включающие денежные требования, возможность осуществления прав по эмиссионным ценным бумагам, права участия в капитале непубличного акционерного общества, право требовать передачи эмиссионных ценных

---

[1] См.: Бохан А. П., Лиманцева Т. И. Правовое регулирование компьютерной информации как объекта уголовно-правовой охраны // Юристъ-Правоведъ. 2015. № 3 (70). С. 38–42.

[2] Общепринятой считается позиция, согласно которой предметом хищения может быть только имущество, отвечающее вещному (имеет определенную физическую форму); экономическому (обладает объективной экономической стоимостью); юридическому (чужое для виновного) признакам.

[3] См.: Архипов А. В. Ответственность за хищение безналичных и электронных денежных средств: новеллы законодательства // Уголовное право. 2018. № 3. С. 4–9.

бумаг, предусмотренные решением о выпуске цифровых финансовых активов, выпуск, учет и обращение которых возможны только путем внесения (изменения) записей в информационную систему на основе распределенного реестра, а также в иные информационные системы». Из определения, закрепленного в ч. 3 ст. 1 Федерального Закона № 259-ФЗ, вытекает ряд признаков цифровой валюты:

- представляет собой совокупность электронных данных (цифрового кода или обозначения);
- существует в безналичной, электронно-цифровой форме и содержится в информационной системе;
- может быть принята в качестве средства платежа, не являющегося денежной единицей РФ, иностранного государства и (или) международной денежной или расчетной единицей, но при этом может быть принята в качестве инвестиций;
- в отношении цифровой валюты отсутствует лицо, обязанное перед их обладателем, за исключением оператора и (или) узлов информационной системы, обязанных обеспечивать соответствие порядка выпуска электронных данных и осуществления в их отношении действий по внесению (изменению) записей в такую информационную систему.

На основании ч. 11 ст. 1 Федерального закона № 259-ФЗ можно сделать вывод, что цифровые финансовые активы и цифровые валюты имеют особую правовую природу и не являются безналичными или электронными денежными средствами, а также не относятся к бездокументарным ценным бумагам, то есть законодатель расширил понятие и виды цифровых прав: к ним относятся не только утилитарные цифровые права, существующие в рамках цифровой инвестиционной платформы, но и финансовые активы – денежные требования, права по эмиссионным ценным бумагам, право требовать передачи эмиссионных ценных бумаг. К цифровым финансовым активам относятся и корпоративные права – право участия в капитале непубличного акционерного общества. Основное различие можно представить следующим образом: **наличные денежные средства выпускаются в виде банкнот, каждая из которых имеет уникальный номер, а безналичные – существуют в виде записей на счетах в банках, а цифровой рубль имеет форму кода в специальном электронном кошельке, открытом в платежной системе Банка России.**

Квалификация деяний, связанных хищением криптовалюты (регулирование которой было предусмотрено в проекте № 259-ФЗ, однако

впоследствии «выпавшее» из него), наиболее успешным примером которой является «биткоин», в настоящее время вызывает определенные сложности. Следует согласиться с А. А. Попиковым, что «виртуальная экономика – составная часть инновационной экономики, а Bitcoin является финансовым инструментом виртуальной, инновационной экономики»[1]. Возвращаясь к признакам предмета хищения, отметим, что экономический признак свойственен криптовалюте, так как есть курс «биткоина» к официальным валютам, существует возможность использования криптовалюты как средства платежа за товары или услуги (на Amazon, Ebay). Юридический признак также присущ криптовалюте, поскольку, несмотря на обезличенность электронных кошельков, они принадлежат определенному пользователю и является чужим для всех остальных.

Судебная практика о хищении криптовалют показывает, что правоприменители преимущественно отказывают в возбуждении уголовных дел, так как в традиционном понимании отсутствует предмет хищения. Например, Н. С. Шатихина полагает, что современное уголовное право использует узкое понимание имущества, поэтому криптовалюту к нему нельзя отнести, как нельзя отнести и к платежным средствам[2]. Э. Л. Сидоренко ссылается на то, что криптовалюта не может быть объектом гражданских прав ввиду отсутствия правовых гарантий для участников сделки, следовательно, нет состава кражи[3]. Такую позицию можно встретить и в иных отраслях права. Например, Арбитражный суд г. Москвы указывает, что криптовалюта не относится к объектам гражданских прав и находится вне правового поля РФ, так как ее правовая природа законодателем не определена[4].

Тем не менее мы полагаем, что наиболее правильно и дальновидно рассматривать криптовалюту как иное имущество[5], а, следовательно,

---

[1] См.: Попиков А. А. Криптовалюта Bitcoin как финансовый инструмент виртуальной экономики // Вопросы инновационной экономики. 2016. № 2. С. 89.

[2] См.: Шатихина Н. Несколько ремарок к вопросу о криптовалюте как предмете хищения. URL: https://zakon.ru/blog/2017/10/18/neskolko_remarok_k_voprosu_o_kriptovalyute_kak_predmete_hischeniya#comment_415739 (дата обращения: 16.01.2021).

[3] См.: Сидоренко Э. Л. Криминальное использование криптовалюты: международные оценки. URL: http://lexandbusiness.ru/view-article.php?id=8675 (дата обращения: 16.01.2021).

[4] См.: Коренная А. А., Тыдыкова Н. В. Криптовалюта как предмет и средство совершения преступлений // Всероссийский криминологический журнал. 2019. Т. 13. № 3. С. 409.

[5] См.: Егорова М. А., Кожевина О. В. Место криптовалюты в системе объектов гражданских прав // Актуальные проблемы российского права. 2020. Т. 15. № 1 (110). С. 81–91.

распространять на нее уголовно-правовую защиту. В судебной практике данная тенденция, учитывая опыт зарубежных стран, только начинает получать свое развитие. Например, Постановлением арбитражного апелляционного суда от 7 мая 2018 года криптовалюта была включена в конкурсную массу должника и определена именно как иное имущество[1].

Также стоит отметить, что в Конвенции против транснациональной организованной преступности 2000 года под имуществом понимаются «любые активы, материальные или нематериальные, движимые или недвижимые, выраженные в вещах или в правах, а также юридические документы или акты, подтверждающие право на такие активы или интерес в них»[2]. Кроме того, сложно не согласиться с мнением В. В. Хилюты о том, что уголовное право охраняет фактически сложившиеся общественные отношения независимо от наличия соответствующих конструкций в цивилистике[3]. ЕСПЧ в одном из решений отметил, что теория собственности не ограничивается материальными вещами[4]: для определения принадлежности какого-то объекта объектом права собственности, необходимо исходить из финансовых интересов и экономической стоимости[5]. Считаем, что это шаг для формирования нового подхода к пониманию предмета хищений. Еще одним аргументом преодоления общепринятого понимания предмета хищения является форма криптовалюты – цифровой код (что уже свойственно для цифровой валюты). Кроме того, в судебной и следственной практике безналичные денежные средства признаются предметом хищений, несмотря на отсутствие физического признака и специфическую форму, о чем было сказано ранее.

Таким образом, в современных условиях уже созданы предпосылки для постановки вопроса о признании криптовалюты предметом

---

[1] Постановление Девятого арбитражного апелляционного суда от 15.05.2018 года № 09ап-1416/2018 по делу № 40-124668/2017 // СПС «Консультант Плюс».

[2] Конвенция против транснациональной организованной преступности: принята в 15.11. 2000 резолюцией 55/25 на заседании 55-й сессии Генер. Ассамблеи ООН // Собрание законодательства РФ. 2004. № 40. Ст. 3882.

[3] Хилюта В. В. Криптовалюта как предмет хищения (или к вопросу о переформатировании предмета преступлений против собственности) // Библиотека уголовного права и криминологии. 2018. № 2 (26). С. 67–68.

[4] Понятием «имущество» (property) в контексте ст. 1 Протокола № 1 к Конвенции о защите прав человека и основных свобод охватывается все, что обладает экономической ценностью для участников гражданского оборота и допускает переход от одного лица к другому.

[5] Решение Европейского суда по правам человека от 18.09.2007 по вопросу приемлемости жалоб № 25379/04, № 21688/05, № 21722/05 и № 21770/05 // ИПО «Гарант».

хищений, а в условиях отсутствия регулятивного законодательства криптовалюту можно рассматривать как иное имущество при определении предмета киберпреступлений.

Список литературы

1. Архипов А. В. Ответственность за хищение безналичных и электронных денежных средств: новеллы законодательства // Уголовное право. 2018. № 3. С. 4–9.
2. Бохан А. П., Лиманцева Т. И. Правовое регулирование компьютерной информации как объекта уголовно-правовой охраны // Юристъ-Правоведъ. 2015. № 3 (70). С. 38–42.
3. Егорова М. А., Кожевина О. В. *Место криптовалюты в системе объектов гражданских прав* // Актуальные проблемы российского права. 2020. Т. 15. № 1 (110). С. 81–91.
4. Коренная А. А., Тыдыкова Н. В. Криптовалюта как предмет и средство совершения преступлений // Всероссийский криминологический журнал. 2019. Т. 13. № 3. С. 408–415.
5. Попиков А. А. Криптовалюта Bitcoin как финансовый инструмент виртуальной экономики // Вопросы инновационной экономики. 2016. № 2. С. 89–106.
6. Сидоренко Э. Л. Криминальное использование криптовалюты: международные оценки. URL: http://lexandbusiness.ru/view-article.php?id=8675 (дата обращения: 16.01.2021).
7. Хилюта В. В. Криптовалюта как предмет хищения (или к вопросу о переформатировании предмета преступлений против собственности) // Библиотека уголовного права и криминологии. 2018. № 2 (26). С. 58–68.
8. Шатихина Н. Несколько ремарок к вопросу о криптовалюте как предмете хищения. URL: https://zakon.ru/blog/2017/10/18/neskolko_remarok_k_voprosu_o_kriptovalyute_kak_predmete_hischeniya#comment_415739 (дата обращения: 10.02.2021).

Д. Д. Добровольский

АНАЛИЗ ПРИЗНАКА ИСПОЛЬЗОВАНИЯ СЕТИ ИНТЕРНЕТ КАК ЭЛЕМЕНТА ОБЪЕКТИВНОЙ СТОРОНЫ В ДИСПОЗИЦИЯХ НОРМ ОСОБЕННОЙ ЧАСТИ УК РФ

Аннотация: Статья посвящена анализу признака использования информационно-телекоммуникационных сетей, включая сеть Интернет как обязательного и факультативного элемента объективной стороны преступления. Предложены пути решения существующих проблем, возникающих при квалификации деяния по данному признаку.

Ключевые слова: информационно-телекоммуникационные сети, сеть Интернет, способ преступления.

ANALYSIS OF THE SIGN OF USING THE INTERNET AS AN ELEMENT OF THE OBJECTIVE SIDE IN THE DISPOSITIONS OF THE RULES OF THE SPECIAL PART OF THE CRIMINAL CODE OF THE RUSSIAN FEDERATION

Abstract: The article focuses on the most common issues arising from the determination of the nature of the crime in which the internet is a determining or constitutive factor. The article also proposes ways of soling the aforementioned issues.

Keywords: information and telecommunication networks, internet, method of crime.

В последнее время можно все чаще слышать о необходимости регулирования интернет-пространства, об особой общественной опасности преступлений, совершаемых с использованием сети Интернет. Такие заявления зачастую не подтверждены серьезными умозаключениями, но законодатель, поддерживая опасения общества, добавляет в составы Особенной части УК РФ такой признак объективной стороны, как использование информационно-телекоммуникационных сетей, включая сеть Интернет. На сегодняшний день данный признак содержится в 20 нормах Особенной части УК РФ. Для простоты восприятия далее в работе будет употребляться термин «использование сети Интернет» в качестве замены формулировки «использование информационно-телекоммуникационных сетей (включая сеть Интернет)» и ее аналогов. Это связанно, во-первых, с отсутствием единой формулировки данного признака объективной стороны в тексте норм Особенной части УК РФ, а во-вторых, с тем фактом, что абсолютное большинство совершаемых преступлений с использованием указанного способа, совершаются в сети Интернет, как в самой крупной и распространенной информационно-телекоммуникационной сети.

Несмотря на то, что законодатель употребляет в диспозиции норм признак «использование сети Интернет» при описании объективной стороны ряда преступлений, существуют деяния, при совершении которых характерно использование этой Сети, хотя указание на такой способ в самом составе отсутствует. Этот факт не препятствует привлечению к уголовной ответственности лиц, совершивших деяние, указанное в диспозиции рассматриваемых составов с помощью сети Интернет. В абсолютном большинстве составов УК РФ в диспозициях содержится открытый перечень способов совершения преступления, поэтому отсутствие указания на какой-либо способ не является препятствием для привлечения к уголовной ответственности. Тем не менее в отдельных случаях законодатель указывает признак совершения деяния с использованием сети Интернет как в общем составе, так и квалифицированном. Само по себе перечисление ряда типичных способов совершения преступления в диспозициях норм Особенной части УК РФ является мерой вполне утилитарной, так как уголовный закон, как никакой другой, должен быть понятен для максимально широкого круга лиц, но из-за того, что такое уточнение отсутствует в сходных составах, это может создавать дополнительные трудности для восприятия права. В качестве примера следует привести составы преступлений, предусмотренные ст. 148 УК РФ «Нарушение права на свободу совести и вероисповеданий» и ст. 282 УК РФ «Возбуждение ненависти либо вражды, а равно унижение человеческого достоинства». В первом случае указание на сеть Интернет отсутствует, тогда как во втором –использование этой Сети выделено отдельно. Можно привести еще ряд примеров преступлений, которые могут совершаться с использованием сети Интернет, но в диспозиции соответствующих норм указание на это отсутствует, например, ст. 146, ст. 237, ст. 283 УК РФ и др.

Что касается квалифицированного признака использования сети Интернет, то возникает вопрос, почему законодатель рассматривает данный признак как повышающий степень общественной опасности деяния. В первую очередь на что обращается особое внимание, это публичность. Предполагается, что преступления, при совершении которых используется сеть Интернет, воздействуют на неопределенно большое количество лиц, что повышает общественную опасность их деяний. Рассмотрим эту проблему на примере составов квазисоучастия в самоубийстве, которые были приняты на волне моральной паники, возникшей именно из-за влияния посторонних лиц на несовершеннолетних посредством сети Интернет. Статьи 110, 110.1 и 110.2 УК РФ

содержат такие квалифицирующие признаки, как «в публичном выступлении, публично демонстрирующемся произведении, средствах массовой информации или информационно-телекоммуникационных сетях (включая сеть Интернет)». Совершение преступления публично предполагает, что оно совершается в присутствии хотя бы одного третьего лица. Публичная форма доведения до самоубийства значительно повышает общественную опасность преступления. Человек – существо общественное. Публичная оценка приобретает в глазах потерпевшего особое значение[1]. Необходимо отметить, что большинство примеров общественно опасного поведения, из-за которых в УК РФ были введены указанные нормы, заключались в непосредственном воздействии на несовершеннолетнего в личных сообщениях, а «публичность» как признак отсутствовала. Можно сделать вывод, что не любое использование сети Интернет, а только сопряженное с публичностью, может быть основанием для квалификации деяния по данному признаку.

Выделяют и другие причины повышения общественной опасности деяния при использовании сети Интернет как характеристики объективной стороны преступления. Использование информационно-телекоммуникационных сетей, включая сеть Интернет, при совершении преступления повышает его степень общественной опасности за счет упрощения совершения деяния, анонимности преступников, а также массовости, быстроты и глубины проникновения негативного информационного воздействия на общество[2]. Что касается анонимности, то ее присутствие не обязательно. Лицо может совершать преступление и с авторизованного аккаунта, с привязанным номером телефона, настоящим именем и т. д. Рассматриваемые нами составы могут устанавливать уголовную ответственность за выраженное мнение, поэтому такая ситуация вполне может иметь место. Также необходимо отметить, что преступления, совершаемые с использованием сети Интернет, оставляют более устойчивые следы, что усложняет сокрытие такого преступления. Таким образом, в зависимости от конкретной ситуации, признак использования сети Интернет либо должен учитываться, либо не должен. Рассмотрим, насколько целесообразно нахождение данного признака в тексте норм Особенной части УК РФ.

[1] Комментарий к Уголовному кодексу РФ в 4 т. Т. 2. Особенная часть. Разделы VII–VIII. С. 63. URL: https://biblio-online.ru/bcode/434549 (дата обращения: 13.01.2021).

[2] Косарев М. Н. Информационно-телекоммуникационные сети как признак преступления // Вестник уральского юридического института МВД России. Екатеринбург: Уральский юридический институт МВД России. 2014. № 2. С. 56.

Согласно п. 4 Постановления Пленума ВС РФ «О судебной практике по уголовным делам о преступлениях экстремистской направленности» под публичными призывами следует понимать выраженные в любой форме (например, в устной, письменной, с использованием технических средств) обращения к другим лицам с целью побудить их к осуществлению экстремистской деятельности. Вопрос о публичности призывов должен разрешаться судами с учетом места, способа, обстановки и других обстоятельств дела[1]. С учетом такого широкого понимания признака публичности возникает сомнение в необходимости отдельного указания на использование сети Интернет. Например, предлагается отказаться от конкретизации форм публичного совершения преступления, а вместо их оставить формулировку «совершенное публично» без других уточнений[2].

В 2012 году способ использования сети Интернет был добавлен в состав, предусмотренный ст. 282 УК РФ «Возбуждение ненависти либо вражды, а равно унижение человеческого достоинства». В последующие годы к уголовной ответственности по измененной ст. 282 УК РФ был привлечен ряд лиц, что вызвало резкий общественный резонанс. Это привело к последующей декриминализации совершения данного преступления впервые, но поскольку административный деликт имеет уголовно-правовую природу, только менее пенализированный, полной декриминализацией это назвать нельзя. Этот пример еще раз показывает, что не во всех случаях использование сети Интернет свидетельствует о большей общественной опасности содеянного. Считаем, что деяния, заключающиеся в высказывании собственного мнения, не являются общественно опасными, а из-за специфических условий взаимодействия людей в сети Интернет, в том числе либо из-за несерьезного отношения к высказываемому, либо из-за возможной привычки резко высказываться вне интернет-пространства, лицу назначается более суровое наказание, хотя о повышенной общественной опасности в этом случае можно говорить весьма условно. По какой-то причине законодатель не стал указывать использование сети Интернет и СМИ в качестве квалифицирующего признака по данному составу. Многие составы

[1] Постановление Пленума Верховного Суда РФ от 28.06.2011 № 11 (ред. от 20.09.2018) «О судебной практике по уголовным делам о преступлениях экстремистской направленности». URL: http://www.consultant.ru/document/cons_doc_LAW_115712/ (дата обращения: 13.01.2021).

[2] Бычков С. Н. Публичность как признак объективной стороны в преступлениях против личности // Скиф. Вопросы студенческой науки. СПб.: Санкт-Петербургский университет МВД России. 2017. № 2. С. 129.

преступлений, касающиеся осуждения за высказывания, вне сети Интернет было бы тяжело доказать, а в условиях использования такой Сети все доказательства, как уже было отмечено ранее, сохранены.

В составах, где публичность является составообразующим признаком (например, ст. 205.1, 280, 280.1 УК РФ), в качестве квалифицирующего признака выступает использование СМИ либо информационно-телекоммуникационных сетей, в том числе сети Интернет. Получается, что законодатель приравнивает СМИ к любой интернет-площадке, которая может массовостью и не обладать. Деяния, подпадающие под признаки рассматриваемых составов, могут происходить в закрытых группах, каналах, форумах, куда не имеет доступа широкий круг лиц, но вместе с этим будут обладать ограниченной, но публичностью. Но почему в этом случае такое деяние будет иметь повышенную общественную опасность, чем просто публичные действия, представляется неясным.

Таким образом, следует признать, что такой признак объективной стороны деяния, как использование сети Интернет в тексте Особенной части УК РФ не раскрывается должным образом. Внутри этого признака как элемента объективной стороны преступления можно выделить множество отдельных специфических способов, каждый из которых будет свидетельствовать о большей или меньшей степени общественной опасности совершенного деяния. Способ, связанный с публичностью, можно оставить без избыточного уточнения при использовании сети Интернет. Если общественная опасность по тем или иным составам усиливается из-за каких-то иных факторов, где сеть Интернет играет существенную роль, то именно эти обстоятельства и следует указать в статьях Особенной части УК РФ. Необходимо либо более четко раскрывать в тексте Особенной части способ использования сети Интернет, с указанием тех специфических признаков, которые повышают общественную опасность соответствующего деяния, либо не применять формулировку «использование сети Интернет» вовсе, а ограничиться только общими признаками, такими как публичность или использование СМИ.

Список литературы

1. Бычков С. Н. Публичность как признак объективной стороны в преступлениях против личности // Скиф. Вопросы студенческой науки. СПб.: Санкт-Петербургский Университет МВД России. 2017. № 2. С. 126–130.
2. Комментарий к Уголовному кодексу РФ в 4 т. Т. 2. Особенная часть. Разделы VII–VIII. С. 63. URL: https://biblio-online.ru/bcode/434549 (дата обращения: 13.01.2021).

3. Косарев М. Н. Информационно-телекоммуникационные сети как признак преступления // Вестник уральского юридического института МВД России. Екатеринбург: Уральский юридический институт МВД России. 2014. № 2. С. 55–57.
4. Постановление Пленума Верховного Суда РФ от 28.06.2011 № 11 (ред. от 20.09.2018) «О судебной практике по уголовным делам о преступлениях экстремистской направленности». URL: http://www.consultant.ru/document/cons_doc_LAW_115712/ (дата обращения: 13.01.2021).

С. С. Потапова

ИСПОЛЬЗОВАНИЕ КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ КАК СПОСОБ СОВЕРШЕНИЯ ПРЕСТУПЛЕНИЙ ПРОТИВ ЛИЧНОСТИ

Аннотация: В данной статье раскрываются причины распространения преступлений с использованием компьютерных технологий в современном мире. Рассматриваются последствия применения компьютерных технологий при совершении преступлений против личности. Предлагается введение в качестве квалифицирующего признака совершения деяния «с использованием электронных или информационно-телекоммуникационных сетей, в том числе сети Интернет» в иные составы Уголовного кодекса РФ, помимо имеющихся на данный момент.

Ключевые слова: киберпреступление, информационные технологии, уголовное право.

USING COMPUTER TECHNOLOGY AS A WAY OF COMMITTING CRIMES AGAINST A PERSON

Abstract: This article reveals the reasons for the spread of crimes using computer technology in the modern world. The consequences of the use of computer technologies in the commission of crimes against a person are considered. It is proposed to introduce as a qualifying sign of the commission of an act “using electronic or information and telecommunication networks, including the Internet” in other compositions of the Criminal Code of the Russian Federation, in addition to those currently available.

Keywords: cybercrime, information technology, criminal law.

Развитие современного общества XXI века целиком и полностью «пронизано» компьютерными технологиями, без которых существование и функционирование той или иной сферы уже не представляется возможным. Информационные и компьютерные технологии стали «помощниками» не только для решения рабочих вопросов (электронный документооборот, использование электронной почты и т. д.), но и бытовых (онлайн-шоппинг, посещение виртуальных музеев и театров).

Вместе с внедрением компьютерных технологий в жизнь граждан и государства, свое широкое и повсеместное развитие получают преступления, которые совершаются с использованием этих технологий. Чем больше информации попадает в информационное пространство, тем выше риски посягательства против личности, на собственность, а также безопасность общества и государства в целом[1].

Беспрерывное развитие компьютерных и телекоммуникационных технологий влечет за собой рост преступлений, совершаемых с их использованием, о чем свидетельствует статистика. Согласно статистическим данным о преступности, предоставленными МВД России, в период с января по ноябрь 2017 года было зарегистрировано 82 440 преступлений, совершаемых с использованием компьютерных и телекоммуникационных технологий, а с января по ноябрь 2018 года – уже 156 307 аналогичных преступлений, что свидетельствует о росте на 89,6 %[2]. В следующие годы неблагоприятный тренд продолжился, как и прогнозировали эксперты[3].

В научной и юридической среде для обозначения преступлений, совершаемых с использованием компьютерных и телекоммуникационных технологий, употребляются различные термины: «преступления в сфере компьютерной информации», «информационные преступления», «преступления, связанные с компьютерными техническими средствами» и др. Также синонимом к вышеперечисленным понятиям является термин «киберпреступление», который получил широкое распространение в международной научной литературе и СМИ, но в современном российском законодательстве данное понятие не раскрывается.

Говоря о совершении преступлений в данной сфере, необходимо рассматривать их с двух точек зрения: с первой – это преступления, непосредственно совершаемые в компьютерной сфере с использованием особых технологических средств, со второй – преступления против личности, собственности и т. д., то есть широко распространенные, но осуществляемые с применением инновационных средств, в особой

[1] См.: Иванова Л. В. Виды киберпреступлений по российскому уголовному законодательству // Юридические исследования. 2019. № 1. С. 25. URL: https://nbpublish.com/library_read_article.php?id=28600 (дата обращения: 19.01.2021).

[2] Статистика преступности (январь–ноябрь 2018 года); Статистика преступности (январь–ноябрь 2017 года). URL: https://мвд.рф/folder/101762/item/15304733/ (дата обращения: 19.01.2021).

[3] См.: Кобец П. Н., Краснова К. А. Проблемы классификации преступлений, совершаемых с использованием информационно-телекоммуникационных технологий // Правоохранительная деятельность органов внутренних дел в контексте современных научных исследований. Материалы Международной научно-практической конференции / Сост. Д. В. Попов. СПб., 2018. С. 178–181.

социально-технологической среде[1]. Обращаясь к теме данной научной статьи, более детальному рассмотрению подвергнется вторая точка зрения из вышеперечисленных.

Возрастающая статистика о преступлениях, совершенных с использованием компьютерных технологий, в цифровом пространстве обусловлена не только развитием данной сферы, но и более гарантированным достижением преступной цели, поскольку такой способ облегчает виновному процесс совершения преступления. Следовательно, использование компьютерных технологий как способа совершения преступлений повышает общественную опасность содеянного и влечет назначение более строгого наказания.

Проблема современного уголовного законодательства заключается в том, что данный признак, ужесточающий меру уголовного наказания, содержится лишь в нескольких статьях Уголовного кодекса РФ (далее – УК РФ). В разделе преступлений против личности таковых насчитывается лишь пять: в ст. ст. 110, 110.1, 110.2, 128.1, 151.2 УК РФ.

Совершение такого преступления, как доведение до самоубийства с использованием информационно-телекоммуникационных сетей, является наиболее ярким примером киберпреступления против личности за последние несколько лет[2]. Например, интернет-игра «Синий кит» для несовершеннолетних лиц, прохождение финального уровня которой предусматривало самоубийство игрока. Статистические данные свидетельствуют более чем о ста несовершеннолетних, которые предположительно являлись игроками и погибли в период с 2015 по 2016 год (пик популярности «Синего кита» в России) по разным обстоятельствам[3].

В данной ситуации использование компьютерных технологий и цифрового пространства способствовало воздействию на несовершеннолетних массово, различными методами – от помощи с решением

[1] См.: Бочкин Д. В. Способы совершения компьютерных преступлений и использование информационных технологий как способ совершения преступления // Сибирские уголовно-процессуальные и криминалистические чтения. 2016. № 5 (13). С. 44. URL: https://cyberleninka.ru/article/n/sposoby-sovershe niya-kompyuternyh-prestupleniy-i-ispolzovanie-informatsionnyh-tehnologiy-kak-sposob-sovershe niya-prestupleniya (дата обращения: 19.01.2021).

[2] Ережипалиев Д. И., Краснова К. А. Противодействие кибербуллициду как средство предупреждения суицидов несовершеннолетних // Юристъ-Правоведъ. 2017. № 3 (82). С. 78–84.

[3] Кочкина Э. Л. Определение понятия «киберпреступление». Отдельные виды киберпреступлений // Сибирские уголовно-процессуальные и криминалистические чтения. 2017. № 3 (17). С. 162–169. URL: https://cyberleninka.ru/article/n/opredelenie-ponyati.. (дата обращения: 19.01.2021).

домашнего задания и просмотра видео в Интернете до прямых уговоров с помощью мессенджеров.

Таким образом, благодаря компьютерным технологиям в данную интернет-игру было вовлечено огромное количество людей, достижение чего без цифрового пространства не представилось бы возможным, а также были использованы более действенные способы влияния на подростков, что облегчало «создателям» достижение намеченной цели – суицида.

На современном этапе развития информационного общества использование информационно-телекоммуникационных сетей облегчает совершение преступлений, повышая при этом общественную опасность содеянного, что обуславливает необходимость включить в качестве квалифицирующего признака совершения деяния «с использованием электронных или информационно-телекоммуникационных сетей, в том числе сети Интернет» и в иные составы УК РФ, помимо имеющихся на данный момент. Исключениями в данном случае будут являться преступления, совершение которых с использованием современных технологий невозможно, например, заражение другого лица ВИЧ-инфекцией или совершение любого вида убийства, предусмотренного УК РФ. Включение же такого признака в большинство статей УК РФ позволит дифференцировать уголовную ответственность.

Список литературы

1. Бочкин Д. В. Способы совершения компьютерных преступлений и использование информационных технологий как способ совершения преступления // Сибирские уголовно-процессуальные и криминалистические чтения. 2016. № 5 (13). С. 40–46. URL: https://cyberleninka.ru/article/n/sposoby-sovershheniya-kompyuternyh-prestupleniy-i-ispolzovanie-informatsionnyh-tehnologiy-kak-sposob-sovershheniya-prestupleniya (дата обращения: 19.01.2021).
2. Ережипалиев Д. И., Краснова К. А. Противодействие кибербуллициду как средство предупреждения суицидов несовершеннолетних // Юристъ-Правоведъ. 2017. № 3 (82). С. 78–84.
3. Иванова Л. В. Виды киберпреступлений по российскому уголовному законодательству // Юридические исследования. 2019. № 1. С. 25–33. URL: https://nbpublish.com/library_read_article.php?id=28600 (дата обращения: 19.01.2021).
4. Кобец П. Н., Краснова К. А. Проблемы классификации преступлений, совершаемых с использованием информационно-телекоммуникационных технологий // Правоохранительная деятельность органов внутренних дел в контексте современных научных исследований. Материалы международной научно-практической конференции / Сост. Д. В. Попов. СПб., 2018. С. 178–181.
5. Кочкина Э. Л. Определение понятия «киберпреступление». Отдельные виды киберпреступлений // Сибирские уголовно-процессуальные и криминалистические чтения. 2017. № 3 (17). С. 162–169. URL: https://cyberleninka.ru/article/n/opredelenie-ponyati.. (дата обращения: 19.01.2021).

Д. П. Король

НЕСОВЕРШЕННОЛЕТНЕЕ ЛИЦО КАК СУБЪЕКТ ПРЕСТУПЛЕНИЙ В СЕТИ ИНТЕРНЕТ

Аннотация: Статья затрагивает вопросы, связанные с таким субъектом преступлений в сети Интернет, как несовершеннолетние лица. Статья посвящена выявлению причины совершения несовершеннолетними лицами преступлений в сети Интернет, а также рассмотрению основных преступлений, которые могут ими совершаться в сети Интернет. Приводятся примеры из судебной практики, подтверждающие данные позиции. Выявляются проблемы правового регулирования и предлагаются пути их решения.

Ключевые слова: несовершеннолетний, преступление, Интернет, информационные технологии, субкультуры.

A MINOR AS A SUBJECT OF CRIMES ON THE INTERNET

Abstract: The article examines issues related to such a subject of crimes on the Internet as minors. The article is devoted to identifying the reasons for committing crimes by minors on the Internet, as well as examining the main crimes that they can commit on the Internet. Examples from judicial practice are given, confirming these positions. The problems of legal regulation on the research topic are identified and ways of their solution are proposed.

Keywords: minor, crime, Internet, information technology, subcultures.

Развитие информационных технологий способствует не только упрощению общественных отношений, коммуникации между людьми, совершенствованию темпов развития экономики, но и росту совершения преступления посредством использования сети Интернет[1]. При этом все чаще в криминальную деятельность вовлекаются несовершеннолетние, поскольку именно они составляют большую часть пользователей информационно-телекоммуникационных технологий, и они более подвержены влиянию каких-то асоциальных идей, которые могут пропагандироваться в открытом доступе в сети Интернет. Несовершеннолетних легко вовлечь в различные деструктивные молодежные субкультуры с помощью сети Интернет, поскольку современное поколение достаточно сильно подвержено влиянию различных социальных сетей, а их измененная психика способствует согласию на различные авантюры, в том числе на те, которые имеют уголовно-правовую направленность[2].

[1] См.: Решняк М. Г. Современные проблемы действия уголовного законодательства России и отдельных зарубежных стран, связанные с цифровизацией преступной деятельности // Безопасность бизнеса. 2020. № 6. С. 54–61.

[2] См.: Кобец П. Н., Краснова К. А. Совершенствование законотворческой деятельности – важнейший фактор предупреждения угрозы экстремизма со стороны тоталитарных сект деструктивного характера // Актуальные проблемы преду-

В связи с этим представляется, что исследование вопросов, связанных с несовершеннолетними лицами как субъектами преступлений в сети Интернет, является актуальным и востребованным.

В период развития общественных отношений под влиянием социальных сетей молодежь оказывается самой неустойчивой и подвижной социальной группой, которая наиболее подвержена различным провокациям, в том числе и уголовно-правового характера.

Несовершеннолетние, находясь в состоянии переходного периода, пребывают в постоянном выборе между ценностями, которые даже нельзя назвать сопоставимыми, они скорее наоборот, взаимоисключающие. В связи с этим у такой категории субъектов зачастую возникают внутренние конфликты, которые активно распространяются деструктивными субкультурами или контркультурами, особенно популярными в сети Интернет, поскольку именно там осуществляется их широкая пропаганда. Иными словами, подрастающее поколение ищет понимания своих интересов, оно в поиске себя, а старшее поколение не всегда способно их понять, услышать и наставить на правильный путь, поэтому несовершеннолетние ищут поддержку и единомышленников среди других людей. Они становятся в группе риска, поскольку в переходном возрасте достаточно легко подвержены различным авантюрам, хотят попробовать что-то новое, что не всегда происходит в положительном аспекте. Такую поддержку они могут увидеть в различных деструктивных субкультурах или контркультурах, поэтому несовершеннолетних достаточно просто вовлечь, когда они находятся в таком состоянии[1].

Сама по себе контркультура представляет собой субкультуру, резко отличающуюся от господствующей культуры и являющуюся прямым вызовом ей. Она представляет собой полное, радикальное отрицание официальной культуры, выступает как средство разрушения ее содержания и форм[2].

Безусловно, что общественные отношения настолько разнообразны, что общество делится зачастую на различные группы, так

преждения экстремизма в молодежной среде. Материалы межведомственной научно-практической конференции. Ульяновск, 2009. С. 196–201.

[1] См.: Краснова К. А. Предупреждение преступности несовершеннолетних, состоящих в неформальных молодежных группах, в крупных и средних городах России // Экономико-правовые и социально-культурные проблемы развития города. Сборник научных трудов / Ответственный секретарь О. В. Лаврухина. М., 2009. С. 229–245.

[2] См.: Соколова С. С. Молодежные субкультуры в трансформирующемся обществе // Вестник Бурятского государственного университета. 2018. № 3–2. С. 89.

скажем «по интересам», и в этом нет ничего плохого, но до того момента, пока это не противоречит интересам других личностей и не переходит за нормы допустимого в рамках действующего законодательства[1]. Особенно это актуально, когда речь идет о становлении несовершеннолетнего лица субъектом преступления в сети Интернет.

Следовательно, можно констатировать факт того, что в эпоху развития информационно-телекоммуникационных технологий наибольшее развитие и пропаганду деструктивные молодежные субкультуры, экстремистские взгляды набирают в сети Интернет[2]. Многие подростки сейчас подвержены влиянию различных социальных сетей, и большую часть времени они проводят именно там. Новые знакомства, игры, увлечения – сейчас это все происходит в виртуальном мире. При этом, учитывая подверженность несовершеннолетних всевозможным авантюрам, они находятся в зоне риска попадания в группу общения с криминальными интересами.

Кроме того, стоит отметить, что с помощью сети Интернет достаточно быстро распространяется любая информация, поскольку данный ресурс имеет неограниченное количество пользователей[3]. Данные выводы подтверждает также и анализ судебной практики.

Например, Р. В. Шумилкин в социальной сети «Вконтакте» («http://vk.com») сети Интернет, используя ник-нейм «Роман Шумилкин» и аккаунт <данные изъяты>, разместил путем добавления в общедоступный раздел социальной сети ссылку на видеозапись под названием «Русский

---

[1] См.: Кобец П. Н., Краснова К. А. Уголовно-правовые меры обеспечения кибербезопасности в условиях экспонентного роста киберпреступности // Обеспечение общественной безопасности и противодействие преступности: задачи, проблемы и перспективы. Материалы Всероссийской научно-практической конференции в 2 т. 2017. С. 205–208; Кобец П. Н., Краснова К. А. О необходимости совершенствования административной ответственности несовершеннолетних в условиях современной России // Актуальные проблемы борьбы с преступностью на современном этапе. Сборник материалов Всероссийской научно-практической конференции, посвященной 90-летию образования дальневосточного юридического института МВД России. Министерство внутренних дел Российской Федерации, Дальневосточный юридический институт. Хабаровск, 2011. С. 222–229.

[2] См.: Кобец П. Н., Краснова К. А. Основы выработки концептуальной платформы в решении проблемы защиты молодежи от угрозы проникновения в ее среду экстремизма и терроризма // Деятельность правоохранительных органов в современных условиях. Сборник материалов XXIII Международной научно-практической конференции. В 2 т. Иркутск, 2018. С. 68–72.

[3] См.: Никитина И. Ф., Лядова А. С. Противодействие распространению и профилактика радикальной деструктивной идеологии в молодежной среде // Вестник Прикамского социального института. 2019. № 3 (84). С. 41.

стяг – марш жестокой молодости», на которой неустановленный мужчина исполняет песню, начинающуюся со слов: «Бойтесь! В наших сердцах ненависть…» и заканчивающуюся словами: «Нам голос крови сказал: «Мы должны победить!». Данный информационный материал полностью соответствует тексту аудиозаписи с названием «Русский стяг», которая признана экстремистским материалом решением Саровского городского суда Нижегородской области от 02.06.2015 и внесена в Федеральный список экстремистских материалов Министерства юстиции РФ под номером 2963. Таким образом, Р. В. Шумилкин допустил массовое распространение экстремистских материалов, включенных в опубликованный Федеральный список экстремистских материалов, путем хранения на общедоступном разделе социальной сети «http://vk.com», осознавая, что указанные материалы находятся в свободно доступе и могут просматриваться и скачиваться неопределенным кругом лиц. Наличие свободного доступа к экстремистским материалам может привести к возможности их распространения, хранения, в том числе среди несовершеннолетних[1].

В другом примере Киянов С. А. обвиняется в совершении приготовления к организации экстремистского сообщества. Из материалов дела следует, что Киянов С. А., находясь по месту своего жительства в г. Краснодаре, через информационную телекоммуникационную сеть Интернет приступил к приисканию возможных участников планируемого к созданию им экстремистского сообщества, в котором он себе отвел руководящую роль. Так, в апреле 2018 года Киянов С. А., используя собственную страницу «Святослав Сейтар» сайта «ВКонтакте» по адресу: https://vk.com/ id391724491, на почве совместного разделения идей анархизма, негативного отношения к существующему конституционному строю и системе органов государственной власти Российской Федерации, путем обмена текстовыми сообщениям познакомился с гражданами Российской Федерации Бабаевым Р. С., ФИО6 и ФИО7, в отношении которых по признакам преступления, предусмотренного ч. 1 ст. 30, ч. 2 ст. 282.1 УК РФ, в отдельное производство выделены материалы и отказано в возбуждении уголовных дел ввиду отсутствия состава преступления. В дальнейшем, в период с 14.04.2018 по 26.11.2018 Киянов С. А., ФИО8, ФИО6 и ФИО7 общались путем обмена текстовыми и голосовыми сообщениями через интернет-сервис обмена мгновенными сообщениями Telegram

[1] Постановление Дмитровского районного суда г. Костромы от 26.01.2020 по делу № 5-12/2020. URL: http://sudact.ru/regular/doc/8TnbPRvkWtre/ (дата обращения: 16.01.2021).

(далее – Telegram), где Киянов С. А. был зарегистрирован под именем Sejtar Member 1, ФИО8 – Dr. Mr. Frog, ФИО6 – Evgenios Bursanidis и ФИО7 – «Паша Вольф»[1].

Таким образом, представленные примеры из судебной практики показывают, что, как правило, различные экстремистские взгляды, а также деструктивные молодежные субкультуры получают свое развитие с помощью сети Интернет.

Стоит отметить, что в настоящее время уголовная ответственность вовлечения несовершеннолетних в деструктивные молодежные субкультуры является не в полной мере совершенной. Как уже ранее было отмечено, что большое распространение уголовно-правовых взглядов отмечается посредством сети Интернет. Однако законодатель не берет это во внимание, в связи с этим преступные деяния, которые совершаются в сети Интернет, остаются безнаказанными или возникают сложности при их квалификации. На наш взгляд, наличие данных проблем в правовом регулировании указывает на то, что настоящее законодательство нуждается во внесении ряда изменений, которые будут учитывать опасность совершения преступлений посредством сети Интернет.

Только посредством совершенствования правового регулирования и принятия иных мер предотвращения можно добиться снижения уровня преступлений, связанных с совершением и вовлечением в совершение преступлений в сети Интернет несовершеннолетних лиц.

Список литературы

1. Кобец П. Н., Краснова К. А. О необходимости совершенствования административной ответственности несовершеннолетних в условиях современной России // Актуальные проблемы борьбы с преступностью на современном этапе. Сборник материалов Всероссийской научно-практической конференции, посвященной 90-летию образования Дальневосточного юридического института МВД России. Министерство внутренних дел Российской Федерации, Дальневосточный юридический институт. Хабаровск, 2011. С. 222–229.
2. Кобец П. Н., Краснова К. А. Основы выработки концептуальной платформы в решении проблемы защиты молодежи от угрозы проникновения в ее среду экстремизма и терроризма // Деятельность правоохранительных органов в современных условиях. Сборник материалов XXIII международной научно-практической конференции. В 2 т. Иркутск, 2018. С. 68–72.
3. Кобец П. Н., Краснова К. А. Совершенствование законотворческой деятельности – важнейший фактор предупреждения угрозы экстремизма со стороны

[1] Приговор Центрального районного суда г. Хабаровска от 10.05.2018 по делу № 1-160/2018. URL: //sudact.ru/regular/doc/y64X8g4FdPgK/ (дата обращения: 16.01.2021).

тоталитарных сект деструктивного характера // Актуальные проблемы предупреждения экстремизма в молодежной среде. Материалы межведомственной научно-практической конференции. Ульяновск, 2009. С. 196–201.
4. Кобец П. Н., Краснова К. А. Уголовно-правовые меры обеспечения кибербезопасности в условиях экспонентного роста киберпреступности // Обеспечение общественной безопасности и противодействие преступности: задачи, проблемы и перспективы. Материалы Всероссийской научно-практической конференции в 2 т. 2017. С. 205–208.
5. Краснова К. А. Предупреждение преступности несовершеннолетних, состоящих в неформальных молодежных группах, в крупных и средних городах России // Экономико-правовые и социально-культурные проблемы развития города. Сборник научных трудов / Ответственный секретарь О. В. Лаврухина. М., 2009. С. 229–245.
6. Никитина И. Ф., Лядова А. С. Противодействие распространению и профилактика радикальной деструктивной идеологии в молодежной среде // Вестник Прикамского социального института. 2019. № 3 (84). С. 41.
7. Решняк М. Г. Современные проблемы действия уголовного законодательства России и отдельных зарубежных стран, связанные с цифровизацией преступной деятельности // Безопасность бизнеса. 2020. № 6. С. 54–61.
8. Соколова С. С. Молодежные субкультуры в трансформирующемся обществе // Вестник Бурятского государственного университета. 2018. № 3–2. С. 89.

К. А. Спехова

КИБЕРПРЕСТУПНОСТЬ: ИЗБИРАТЕЛЬНОЕ ПРАВОПРИМЕНЕНИЕ

Аннотация: В статье рассмотрены основные проблемы осуществления расследования киберпреступлений. Сделан вывод о том, что неэффективность системы борьбы с киберпреступностью не в последнюю очередь связана с тем, что сотрудники правоохранительных органов, руководствуясь мотивами более быстрого карьерного роста, путем достижения требуемых руководством показателей раскрываемости, концентрируются на расследовании так называемых «экстремистских» преступлений в Сети, в то время как реальные преступления с высокой степенью общественной опасности фактически не расследуются, в связи с намного большей трудоемкостью расследования таких преступлений.

Ключевые слова: киберпреступность, преступления в Интернете, экстремистские преступления, TOR, борьба с киберпреступностью.

CYBERCRIME: SELECTIVE ENFORCEMENT

Abstract: The article considers the main problems of the investigation of cybercrimes. It was concluded that the ineffectiveness of the system of fighting cybercrime is not least due to the fact that law enforcement officers, guided by the motives of achieving

the fastest possible career growth, concentrate on investigating the so-called “extremist” crimes on the Internet, meanwhile real crimes with a high degree of public danger are not investigated, due to the much greater labour intensity of the investigation of such crimes.

*Keywords***:** cybercrime, crimes on the Internet, extremist crimes, TOR, fighting cybercrime.

Развитие информационных технологий и диджитализация общества имеет свою обратную сторону – увеличение количества преступлений, совершенных в Сети[1]. За 2020 год количество киберпреступлений в Российской Федерации увеличилось на 94,5 % по сравнению с 2019 годом[2]. При этом киберпреступность увеличивается не только количественно, но и качественно, создавая все новые формы преступной деятельности[3]. На сегодняшний день преступность в Интернете фиксируется в огромном количестве форм, при этом наблюдается сращивание онлайн- и офлайн-преступности. С помощью системы TOR существует возможность воспользоваться нелегальными услугами так называемого «даркнета»: заказать наркотики или даже нанять киллера[4]. При этом, как справедливо отмечает Г. А. Гундерич, даже фиксируемое увеличение киберпреступности не в полной мере отвечает реальному положению дел, учитывая высокую латентность киберпреступности, а также несовершенство систем учета преступлений в Российской Федерации[5].

Согласно обзору Банка России в правоохранительные органы при несанкционированных операциях с использованием платежных карт обращались только 4 % потерпевших физических лиц и 20 %

---

[1] См.: Кобец П. Н., Краснова К. А. Проблемы классификации преступлений, совершаемых с использованием информационно-телекоммуникационных технологий // Правоохранительная деятельность органов внутренних дел в контексте современных научных исследований. Материалы Международной научно-практической конференции / Сост. Д. В. Попов. СПб., 2018. С. 178–181.

[2] Число киберпреступлений в России выросло на 94,6 % за 2020 год. URL: https://ru-bezh.ru/gossektor/news/20/12/02/chislo-kiberprestuplenij-v-rossii-vyiroslo-na-946-proczentov-za (дата обращения: 10.02.2021).

[3] См.: Кобец П. Н., Краснова К. А. Уголовно-правовые меры обеспечения кибербезопасности в условиях экспонентного роста киберпреступности // Обеспечение общественной безопасности и противодействие преступности: задачи, проблемы и перспективы. Материалы Всероссийской научно-практической конференции в 2 т. Краснодар, 2017. С. 205–208.

[4] Узденов Р. М. Новые границы киберпреступности // Всероссийский криминологический журнал. 2016. № 4. URL: https://cyberleninka.ru/article/n/novye-granitsy-kiberprestupnosti (дата обращения: 07.01.2021).

[5] Гундерич Г. А. Состояние киберпреступности // Научный вестник Крыма. 2018. № 4 (15). URL: https://cyberleninka.ru/article/n/sostoyanie-kiberprestupnosti (дата обращения: 07.01.2021).

потерпевших юридических лиц[1]. При этом такая латентность связана не только с объективными факторами, но и субъективным нежеланием многих сотрудников правоохранительных органов возбуждать дела, связанные с совершением преступлений в Сети, так как такие дела «портят статистику» (в силу сложности их раскрытия и большого объема работы, а также нехватки специальных знаний) правоохранительных органов, что приводит к ряду проблем (начиная от депримирования и заканчивая увольнением) у сотрудников правоохранительных органов.

Исходя из вышеизложенного, очевидно, что киберпреступность представляет собой реальную угрозу не только правам и имущественным интересам отдельных граждан, но и национальной безопасности Российской Федерации, учитывая масштабность данного преступного явления и его негативное влияние на общее состояние законности в Российской Федерации.

Вместе с тем следует констатировать, что существующее положение дел в Российской Федерации не позволяет предполагать стабилизацию ситуации с киберпреступностью[2].

Следует отметить, что сложности противодействия киберпреступности имеют часто объективный характер. Как справедливо отмечает В. В. Тулегенов, киберпреступность является формой выражения криминального профессионализма, так как для большинства преступлений в этой сфере требуется серьезная профессиональная подготовка[3]. При этом для расследования таких преступлений зачастую необходима не меньшая профессиональная подготовка, что создает объективные сложности для органов осуществления досудебного расследования, а также оперативно-розыскных органов в борьбе с реальными киберпреступлениями[4].

---

[1] Трофимова Д. Н. Киберпреступность в Российской Федерации: пути предупреждения // Молодой ученый. 2020. № 15 (305). С. 259–261. URL: https://moluch.ru/archive/305/68693/ (дата обращения: 13.01.2021).

[2] См.: Решняк М. Г. Современные проблемы действия уголовного законодательства России и отдельных зарубежных стран, связанные с цифровизацией преступной деятельности // Безопасность бизнеса. 2020. № 6. С. 54–61.

[3] Тулегенов В. В. Киберпреступность как форма выражения криминального профессионализма // Криминология: вчера, сегодня, завтра. 2014. № 2 (33). URL: https://cyberleninka.ru/article/n/kiberprestupnost-kak-forma-vyrazheniya-kriminalnogo-professionalizma (дата обращения: 07.01.2021).

[4] См.: Кобец П. Н., Краснова К. А. О роли МВД России в обеспечении общественной безопасности // Вопросы совершенствования деятельности милиции общественной безопасности. Сборник. Всероссийский научно-исследовательский институт МВД РФ. М., 2009. С. 57–65.

Очевидно, что не меньшей проблемой является то обстоятельство, что фокус борьбы с преступлениями в Сети направлен прежде всего на выявление преступлений так называемой «экстремистской» направленности, связанной с распространением в социальных сетях информации с помощью «лайков» и «репостов»[1].

Столь пристальное внимание сотрудников правоохранительных органов к расследованию таких преступлений легко объяснимо. Для расследования ряда киберпреступлений (например, связанных с действиями международных хакерских групп по промышленному и государственному шпионажу) необходима соответствующая квалификация, а также наличие специального, дорогостоящего оборудования. В отличие от вышеуказанных киберпреступлений, борьба с «лайками» и «репостами» не требует сбора серьезной доказательной базы. Так, у жительницы Барнаула Марии Мотузной было обнаружено 13 сохраненных «мемов» на странице в социальной сети «ВКонтакте». По мнению правоохранительных органов, данные «мемы», в том числе и «демотиваторы», показывающие священнослужителей с отрицательной стороны», имели признаки экстремизма, вследствие чего в отношении М. Мотузиной было возбуждено уголовное дело за экстремизм и оскорбление чувств верующих[2]. При этом вся доказательная база по таким делам состоит из нескольких скриншотов предполагаемого правонарушения, выводов лингвистической экспертизы и протокола допроса подозреваемого (обвиняемого). Более того, как показывает практика, суды крайне формально относятся к собранным по делу доказательствам, фактически повторяя фабулу обвинительного заключения.

К сожалению, следует отметить, что практика работы правоохранительных органов, в частности – механизм оценки эффективности сотрудника правоохранительного органа, отличается чрезвычайно высоким уровнем формализма[3]. По сути дела, сотруднику правоохранительного органа

[1] См.: Кобец П. Н., Краснова К. А. Основы выработки концептуальной платформы в решении проблемы защиты молодежи от угрозы проникновения в ее среду экстремизма и терроризма // Деятельность правоохранительных органов в современных условиях. Сборник материалов XXIII Международной научно-практической конференции. В 2 т. 2018. С. 68–72.

[2] См.: Олейникова П. А. Уголовная ответственность за лайки и репосты – проблемы квалификации и наказание за содеянное // E-Scio. 2020. № 7 (46). URL: https://cyberleninka.ru/article/n/ugolovnaya-otvetstvennost-za-layki-i-reposty-problemy-kvalifikatsii-i-nakazanie-za-sodeyannoe (дата обращения: 07.01.2021).

[3] См.: Кобец П. Н., Краснова К. А. Основы выработки концептуальной платформы в решении проблемы предотвращения и защиты молодежи от угрозы проникновения в ее среду экстремизма и терроризма // Философия права. 2018. № 2 (85). С. 74–79.

намного выгоднее расследовать несколько «тяжких» (по классификации УК РФ) дел экстремистского характера о «лайках» и «репостах» в социальных сетях (даже при условии отсутствия критерия реальной общественной опасности), чем заниматься расследованием сложных киберпреступлений, расследование которых требует серьезной профессиональной подготовки сотрудника правоохранительного органа и может затянуться на несколько месяцев. К преступлениям такого рода следует отнести:

1. Хакерское мошенничество, которое ряд преступников воспринимают как своеобразный вид спорта[1].
2. Финансовые махинации, захват собственности и ценностей в Интернете.
3. Угроза внешних интервенций, наличие угроз для атомных электростанций, системы ядерного оружия РФ и т. д.
4. Использование «даркнета» для подготовки офлайн-преступлений.
5. Отмывание денежных средств с помощью криптовалют и иных онлайн-инструментов.

Именно на выявлении (учитывая их высокую латентность и общественную опасность) и расследовании данных преступлений прежде всего должны сконцентрироваться отечественные правоохранительные органы, в то время как вопросы уголовной ответственности за «лайки» и «репосты», учитывая наличие столь существенных угроз, не должны быть безусловным приоритетом при расследовании уголовных преступлений в Сети.

Резюмируем. Недостаточное внимание правоохранительных органов к расследованию киберпреступлений будет сохраняться и дальше, превращая российский сегмент Интернета во все более опасную для пользователей среду. Лишь комплексное изменение подходов правоохранителей в борьбе против киберпреступности, приоритизация расследований преступлений с материальным составом и реальный учет общественной опасности расследуемых преступлений при оценке квалификации правоохранителей могут изменить вышеуказанную негативную тенденцию.

Список литературы

1. Гундерич Г. А. Состояние киберпреступности // Научный вестник Крыма. 2018. № 4 (15). URL: https://cyberleninka.ru/article/n/sostoyanie-kiberprestupnosti (дата обращения: 07.01.2021).

[1] См.: Овчинский А. С., Шмонин А. В., Торопов Б. А., Васильев Ф. П. Криминальная среда цифрового мира как угроза кибербезопасности // Вопросы безопасности. 2019. № 5. URL: https://cyberleninka.ru/article/n/kriminalnaya-sreda-tsifrovogo-mira-kak-ugroza-kiberbezopasnosti (дата обращения: 10.01.2021).

2. Кобец П. Н., Краснова К. А. Основы выработки концептуальной платформы в решении проблемы защиты молодежи от угрозы проникновения в ее среду экстремизма и терроризма // Деятельность правоохранительных органов в современных условиях. Сборник материалов XXIII международной научно-практической конференции. В 2 т. 2018. С. 68–72.
3. Кобец П. Н., Краснова К. А. О роли МВД России в обеспечении общественной безопасности // Вопросы совершенствования деятельности милиции общественной безопасности. Сборник. Всероссийский научно-исследовательский институт МВД РФ. М., 2009. С. 57–65.
4. Кобец П. Н., Краснова К. А. Основы выработки концептуальной платформы в решении проблемы предотвращения и защиты молодежи от угрозы проникновения в ее среду экстремизма и терроризма // Философия права. 2018. № 2 (85). С. 74–79.
5. Кобец П. Н., Краснова К. А. Проблемы классификации преступлений, совершаемых с использованием информационно-телекоммуникационных технологий // Правоохранительная деятельность органов внутренних дел в контексте современных научных исследований. Материалы международной научно-практической конференции / Сост. Д. В. Попов. СПб., 2018. С. 178–181.
6. Кобец П. Н., Краснова К. А. Уголовно-правовые меры обеспечения кибербезопасности в условиях экспонентного роста киберпреступности // Обеспечение общественной безопасности и противодействие преступности: задачи, проблемы и перспективы. Материалы Всероссийской научно-практической конференции в 2 т. Краснодар, 2017. С. 205–208.
7. Овчинский А. С., Шмонин А. В., Торопов Б. А., Васильев Ф. П. Криминальная среда цифрового мира как угроза кибербезопасности // Вопросы безопасности. 2019. № 5. URL: https://cyberleninka.ru/article/n/kriminalnaya-sreda-tsifrovogo-mira-kak-ugroza-kiberbezopasnosti (дата обращения: 10.01.2021).
8. Олейникова П. А. Уголовная ответственность за лайки и репосты – проблемы квалификации и наказание за содеянное // E-Scio. 2020. № 7 (46). URL: https://cyberleninka.ru/article/n/ugolovnaya-otvetstvennost-za-layki-i-reposty-problemy-kvalifikatsii-i-nakazanie-za-sodeyannoe (дата обращения: 07.01.2021).
9. Решняк М. Г. Современные проблемы действия уголовного законодательства России и отдельных зарубежных стран, связанные с цифровизацией преступной деятельности // Безопасность бизнеса. 2020. № 6. С. 54–61.
10. Трофимова Д. Н. Киберпреступность в Российской Федерации: пути предупреждения // Молодой ученый. 2020. № 15 (305). С. 259–261. URL: https://moluch.ru/archive/305/68693/ (дата обращения: 13.01.2021).
11. Тулегенов В. В. Киберпреступность как форма выражения криминального профессионализма // Криминология: вчера, сегодня, завтра. 2014. № 2 (33). URL: https://cyberleninka.ru/article/n/kiberprestupnost-kak-forma-vyrazheniya-kriminalnogo-professionalizma (дата обращения: 07.01.2021).
12. Узденов Р. М. Новые границы киберпреступности // Всероссийский криминологический журнал. 2016. № 4. URL: https://cyberleninka.ru/article/n/novye-granitsy-kiberprestupnosti (дата обращения: 07.01.2021).

Р. О. Поспех

МОШЕННИЧЕСТВО В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ КАК ВИД МОШЕННИЧЕСТВА

Аннотация: Автор рассматривает уголовно-правовые проблемы противодействия мошенничеству в сфере компьютерной информации. Особое внимание уделяется исследованию предмета и новейших способов совершения рассматриваемого преступления. Делается вывод о самостоятельности данного состава и необходимости его сохранения в действующем уголовном законе.

Ключевые слова: киберпреступность, мошенничество, компьютерная информация, социальная инженерия, электронные торги.

FRAUD IN THE FIELD OF COMPUTER INFORMATION AS A TYPE OF FRAUD

Abstract: The author examines the criminal law problems of combating fraud in the field of computer information. Particular attention is paid to the study of the subject and the latest methods of committing the crime in question. The conclusion is made about the independence of this composition and the need to preserve it in the current criminal law.

Keywords: cybercrime, fraud, computer information, social engineering, electronic trading.

Современный мир сложно представить без высоких технологий, которые пронизывают уже абсолютно все сферы государственной и общественной жизни, происходит глобальная информатизация общества. Данный процесс имеет как положительный, так и отрицательный результат. Одно из проявлений отрицательной стороны развития высоких технологий – использование последней в криминальной сфере, порождающее новые виды преступлений и преступности, которые причиняют вред общественным интересам в сфере компьютерной информации и информационных технологий, телекоммуникационных сетей связи. В период пандемии наибольшее распространение приобрели мошенничества, связанные с банковскими картами, банковскими счетами, персональными данными, совершаемые посредством телефонной связи, удаленно, без непосредственного очного контакта с мошенником.

Новые способы мошенничества вызывают необходимость совершенствования уголовного законодательства, устанавливающего ответственность за совершение мошенничества. На современном этапе развития России важность квалификации мошенничества как формы хищения приобретает особое значение. Появляются различные способы обмана доверчивых граждан, изъятия у них средств и другого имущества

обманным путем. В информационный век это наказуемое деяние приобретает совсем иную форму, отличную от классического, привычного нам мошенничества[1].

Статья 159 Уголовного кодекса Российской Федерации от 13 июня 1996 года № 63-ФЗ (далее – УК РФ) определяет мошенничество как хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием. В доктрине уголовного права отсутствует единое понимание мошенничества и отнесение его к формам хищения. Отдельные авторы, например Н. А. Лопашенко[2], полагают, что мошенничество относится к формам хищения в силу традиции, другие авторы оспаривают традиционное представление и не считают мошенничество формой хищения. Мы придерживаемся традиционной точки зрения.

В связи с развитием новых видов мошенничества законодателем была проведена ревизия действующего законодательства, и в 2012 году в УК РФ были внесены изменения, интегрирующие в правовое поле новые составы мошенничества, включающие мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ). Согласно ст. 159.6 УК РФ мошенничество в сфере компьютерной информации представляет собой хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей. Важно отметить, что по составу данной статьи компьютерная информация выступает средством осуществления преступления.

В результате указанных изменений, внесенных законодателем в УК РФ в 2012 году, для правоприменителя была установлена некая конкуренция уголовно-правовых норм, устанавливающих уголовную ответственность за мошенничество. Изучение признаков составов преступлений, закрепленных ст. 159.1–159.6 УК РФ, приводит к такому выводу, что эти нормы являются специальными по отношению к общей норме о мошенничестве (ст. 159 УК РФ).

---

[1] См.: Ступникова А. М., Картавченко В. В. Понятие мошенничества в России, как формы хищения (уголовно-правовой аспект) // Право. Нормотворчество. Закон: межд. науч.-практ. конференция. Самара, 2018. С. 150.

[2] См.: Лопашенко Н. А. Законодательная реформа мошенничества: вынужденные вопросы и вынужденные ответы // Криминологический журнал БГУЭП. 2015. Т. 9. № 3. С. 504.

Правила квалификации при таком виде конкуренции предусмотрены ч. 3 ст. 17 УК РФ: «Если преступление предусмотрено общей и специальной нормами, то совокупность преступлений отсутствует, и уголовная ответственность наступает по специальной норме». Таким образом, состав преступления, предусмотренный ст. 159.6 УК РФ, квалифицируемый как мошенничество в сфере компьютерной информации, является специальным по отношению к составу мошенничества, предусмотренному ст. 159 УК РФ. Вместе с тем на практике возникает ряд вопросов, является ли состав преступления, предусмотренный ст. 159.6 УК РФ, – мошенничеством.

В настоящее время наиболее распространены следующие способы мошенничества в сфере компьютерной информации[1]:

1. Неправомерное завладение регистрационными данными разных учетных записей (googlemarket, appstore и т. п.) для последующей их реализации, дальнейшего использования при совершении мошеннических действий.
2. Социальный инжиниринг. Его использование связано с применением компьютера или телефона для получения доступа к счету, упрощения такого доступа либо получения необходимой информации для хищения персональных данных.
3. Распространение вредоносного программного обеспечения (ПО), которое блокирует возможность использования компьютера либо затрудняет его использование. Для разблокировки мошенники предлагают получить код с отправкой платного SMS, что не гарантирует решение проблемы.
4. Фишинг – способ мошенничества в сфере компьютерной информации, направленный на получение доступа к конфиденциальным данным пользователей: логинам и паролям. Фишинговые письма являются электронными сообщениями от мошенника в форме официального письма от банка, провайдера, которые направляются для получения логина и пароля пользователя к информационной системе.
5. Кардинг – незаконное использование принадлежащей третьим лицам информации о платежных средствах.
6. Использование платежных сервисов интернет-ресурсов при проведении платежных операций с последующим обналичиванием

[1] См.: Жихорев Д. В. Способы совершения мошенничества в сфере компьютерной информации // Преступность в СНГ: проблемы предупреждения и раскрытия преступлений: сб. материалов. Воронеж, 2018. С. 255–256.

денежных средств или покупкой различных товаров с использованием денежных средств, находящихся на счету жертвы (мошенники обладают необходимыми для осуществления транзакции данными карты жертвы).

7. Рассылка разного рода электронных писем на электронные почтовые ящики, текст которых вводит в заблуждение получателя, акцентируя его внимание на необходимости определенного рода платежей.
8. Проведение электронных торгов (с фиктивными лотами) или «интернет-аукционов» (продавцы-мошенники для завышения цены аукционного товара делают на него ставки).
9. Организация через Интернет благотворительных акций, при которой предлагается перечислять денежные суммы на счета конкретных лиц (тяжело больных, нуждающихся в срочных операциях, инвалидов и т. п.).
10. Осуществление взлома электронных кошельков (в частности, путем рассылки вредоносного программного обеспечения или ссылок на него) и последующее хищение денежных средств (их обналичивание), перевод на другие счета, оплата услуг либо товаров через электронные платежные системы.

Рассмотренные способы наиболее часто встречаются в судебной и следственной практике, однако их перечень не является исчерпывающим и может постоянно пополняться.

Как хищение мошенничество имеет следующие признаки[1]:

1. Изъятие имущества на безвозмездной основе, при этом лицо, производящее изъятие, не имеет законных прав на имущество, и изъятие характеризуется как противоправное.
2. Лицо преследует корыстную цель.
3. В результате совершенного деяния причиняется ущерб собственнику или иному законному владельцу имущества.

Вместе с тем некоторые исследователи полагают, что мошенничество в сфере компьютерной информации располагает не всеми признаками общего состава мошенничества. Как уже было сказано выше, обман, злоупотребление доверием и введение потерпевшего в заблуждение являются признаками мошеннических действий, которые неразрывно связаны

[1] См.: Шишкина Н. В. Понятие и виды мошенничества как разновидности преступлений против собственности // Научная дискуссия современной молодежи: актуальные вопросы, достижения и инновации: сб. статей III Межд. науч.-практ. конф: в 2 ч. Пенза, 2018. С. 158.

с преступным намерением лица совершить хищение имущества потерпевшего. При этом заблуждение является прямым следствием искажения истины посредством действий виновного лица. Искажение истины может быть вызвано как совершением активных действий виновного по созданию специально моделируемой ситуации, в результате которой у потерпевшего складывается определенная модель поведения, специально создаваемая виновным с целью завладения имуществом потерпевшего; либо, напротив, без совершения активных действий, так как у потерпевшего уже сложилось искаженное понимание действительности, и любые действия его могут разрушить. Следовательно, заблуждение потерпевшего лежит в плоскости интеллектуальной и волевой деятельности.

При совершении мошенничества в сфере компьютерной информации данная модель может проявляться в следующей форме: потерпевший уверен, что совершает действия, способствующие приросту его имущества – денежных средств – на платежной карте или счету, либо оплате заказанного им товара, либо совершение благотворительных действий и т. д. Совершению мошенничества в сфере компьютерной информации в абсолютном большинстве случаев предшествуют активные действия виновных лиц, которые или методом убеждения воздействуют на потерпевшего, либо предварительно создают «атмосферу», попадая в которую потерпевший вводится в заблуждение.

Заблуждение потерпевшего относительно действий, совершаемых виновным лицом и самим потерпевшим в соответствии с умыслом виновного, может не иметь безоговорочного и окончательного характера – потерпевший может сомневаться в информации или действии преступника. Но если в итоге он совершает действия или принимает решение в соответствии с информацией или действиями, совершаемыми виновным, следует считать, что потерпевший был обманут или введен в заблуждение, соответственно, мошенничество было совершено, а информация, предоставленная преступником, была воспринята потерпевшим как истина. В качестве одного из признаков мошенничества следует назвать то, что потерпевший, обманутый или введенный в заблуждение, совершает добровольные действия, способствующие переходу принадлежащего ему имущества или права на имущество лицу, совершающему преступление. Добровольность таких действий условна, с одной стороны, потерпевшего никто не принуждает совершать такие действия, прямого давления на его волю никто не оказывает, с другой стороны, добровольность обусловлена той искаженной информацией, которая лежит в основе обмана потерпевшего. Иными словами,

с точки зрения потерпевшего, он действует добровольно, без давления со стороны, при этом он не осознает, что его действия – результат психологического манипулирования виновного, иначе, осознавая, что совершаемые в отношении него действия являются обманом, он бы не стал отчуждать свое имущество.

Некоторые исследователи отмечают, что при компьютерном мошенничестве это условие не всегда выполняется, поскольку потерпевший часто узнает о негативных последствиях своих действиях уже значительно позже, к примеру, обнаружив, что с его банковской карты, счета мобильного телефона или иных электронных средств переведены денежные средства. Иными словами, при совершении мошенничества в данной области налицо отсутствие одного из признаков состава преступления – добровольность[1], что ставит под сомнение отнесение данного состава к специальному виду мошенничества. С данной точкой зрения невозможно согласиться по той причине, что при совершении любого вида мошенничества (общего, квалифицированного или специализированного) потерпевший может узнать о совершении в отношении него данного преступления значительно позже, но это не нивелирует то обстоятельство, что в момент совершения мошенничества потерпевший добровольно передавал свое имущество или право на него.

Таким образом, мошенничество в сфере компьютерной информации обладает всеми признаками общего состава мошенничества. Отличием от общего состава, предусмотренного ст. 159 УК РФ, является сфера преступного деяния, где компьютерная информация является средством совершения мошенничества.

Список литературы

1. Безверхов А. Г. Мошенничество и его виды: вопросы законодательной регламентации и квалификации // Уголовное право. 2015. № 5. С. 8–14.
2. Дмитриева Ю. М. Мошенничество в сфере компьютерной информации: виды и проблемы квалификации // Раскрой свой научный потенциал: сб. научных трудов по материалам III Международной научно-практической молодежной конференции. Нижний Новгород, 2017. С. 84–89.
3. Жихорев Д. В. Способы совершения мошенничества в сфере компьютерной информации // Преступность в СНГ: проблемы предупреждения и раскрытия преступлений: сб. материалов. Воронеж, 2018. С. 255–257.

[1] См.: Дмитриева Ю. М. Мошенничество в сфере компьютерной информации: виды и проблемы квалификации // Раскрой свой научный потенциал: сб. научных трудов по материалам III Международной научно-практической молодежной конференции. Нижний Новгород, 2017. С. 85.

4. Лопашенко Н. А. Законодательная реформа мошенничества: вынужденные вопросы и вынужденные ответы // Криминологический журнал БГУЭП. 2015. Т. 9. № 3. С. 504–513.
5. Ступникова А. М., Картавченко В. В. Понятие мошенничества в России как формы хищения (уголовно-правовой аспект) // Право. Нормотворчество. Закон: межд. науч.-практ. конференция. Самара, 2018. С. 150–154.
6. Шишкина Н. В. Понятие и виды мошенничества как разновидности преступлений против собственности // Научная дискуссия современной молодежи: актуальные вопросы, достижения и инновации: сб. статей III Межд. науч.-практ. конф: в 2 ч. Пенза, 2018. С. 157–159.

Г. О. Тамразов

МОШЕННИЧЕСТВО В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ: ПРОБЛЕМЫ КВАЛИФИКАЦИИ

*Аннотация***:** В настоящей статье рассматривается вопрос обоснованности отнесения преступления, предусмотренного ст. 159.6 УК РФ («Мошенничество в сфере компьютерной информации»), к одному из видов мошенничества. Предлагается изменить трактовку данного состава в законе.

*Ключевые слова***:** мошенничество, компьютерная информация.

COMPUTER FRAUD: QUALIFICATION ISSUES

Abstract: This article examines the issue of the validity of the attribution of the crime under Art. 159.6 of the Criminal Code of the Russian Federation (“Fraud in the field of computer information”), to one of the types of fraud. It is proposed to change the interpretation of this composition in the law.

Keywords: fraud, computer information.

В связи с повсеместным внедрением информационных технологий возникает повышенная угроза безопасности как общества в целом, так и интересов отдельной личности, связанных не только с охраной персональных данных, но и защитой собственности, что не может не найти своего отражения в уголовном законе. Необходимость введения новых составов обусловлена изменением обстановки в российском обществе, связанной с развитием рынка товаров и услуг, а также с появлением новых технологий и возможностей гаджетов.

Поскольку преступность опережает развитие уголовного закона, законодатель может только констатировать появление новых видов общественно-опасных деяний и установить за них ответственность,

но для этого нужно, чтобы был накоплен определенный массив таких деяний. Преступники же используют все новые мошеннические уловки, рождаются новые виды мошенничества, с учетом мобильности системы преступности и ее высокой адаптивности к трансформирующейся экономической обстановке, что провоцирует усложнение непосредственных объектов мошенничества. По мнению М. Ф. Мусаеляна, наличие в уголовном законе одной общей нормы, закрепленной в ст. 159 УК РФ, не позволяло надлежащим образом обеспечить защиту интересов граждан, пострадавших от мошеннических действий, так как не в полной мере учитывала особенности тех или иных экономических отношений[1].

Поэтому законодателем были разграничены различные области совершения мошеннических действий и выделены специальные составы мошеннического завладения чужим имуществом, то есть, как указывают специалисты в области уголовного права, «российский законодатель пошел по пути тщательного дифференцированного подхода к определению пределов уголовной ответственности за мошенничество с учетом сферы его совершения и используемых при этом средств и способов»[2].

Естественно, это законодательное решение вызвало множество вопросов по применению новых норм, которые должны разрешаться на практике единообразно.

Диспозиция ст. 159.6 УК РФ устанавливает, что это преступление состоит в хищении чужого имущества или приобретении права на него специфическим способом: путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей.

Однако, учитывая признаки общего состава мошенничества, закрепленные в ст. 159 УК РФ, нужно помнить, что мошенничество в любом случае совершается с использованием обмана или злоупотребления доверием. Применительно же к составу преступления, предусмотренного ст. 159.6, следует признать, что эти элементы объективной стороны, являющиеся обязательными для мошеннического завладения

[1] См.: Мусаелян М. Ф. О некоторых проблемах, связанных с введением в УК РФ специальных составов мошенничества // Российский следователь. 2016. № 10. С. 26.

[2] Журавлева Г. В., Карпова Н. А. Мошенничество в сфере компьютерной информации: спорные вопросы теории и практики // Вестник Московского университета МВД России. 2017. № 5. С. 153.

имуществом или правом на него, не могут иметь места. Ведь потерпевшим от такого деяния является лицо, «обманутое» техническим средством, что само по себе невозможно ввиду отсутствия у технического средства эмоционально-волевого аспекта.

В то же время стоит обратить внимание на п. 1 Постановления Пленума Верховного Суда РФ от 30.11.2017 № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате»[1], сменившего остановление на аналогичную тему десятилетней давности (от 27.12.2007 № 51), в котором специально оговаривается, что обман или злоупотребление доверием как способ совершения преступления характерны для составов, предусмотренных ст.ст. 158.1, 159, 159.1, 159.2, 159.3, 159.5 УК РФ, однако преступление, предусмотренное ст. 159.6 УК РФ, в этом перечне не упоминается. Правомерно ли в таком случае отнесение данного деяния к одному из видов мошенничества?

Например, Афонин был осужден по ч. 2 ст. 159.6 УК РФ за то, что тайно взял из кармана одежды знакомого ему К. телефон с установленной в нем сим-картой. Просмотрев папку СМС-сообщений, Афонин увидел СМС-сообщения со специального номера «900» ПАО «Сбербанк России» о балансе денежных средств, находящихся на лицевом счету карты ПАО «Сбербанк России» на имя К., в результате чего узнал, что к сим-карте сотового оператора, зарегистрированной на имя К., подключена дистанционная финансовая банковская услуга «Мобильный банк». Зная о возможностях управления лицевым счетом карты путем использования подключенной к карте дистанционной финансовой банковской услуги «Мобильный банк», предоставляемой ПАО «Сбербанк России», к номеру сотового телефона на имя К., удостоверившись в наличии денежных средств на лицевом счету карты К., преследуя корыстный умысел, направленный на незаконное обогащение, похитил денежные средства с лицевого счета карты К.[2]

Однако некоторые ученые ссылаются на п. 2 Постановления Пленума Верховного Суда РФ от 27 декабря 2002 года № 29

[1] Постановление Пленума Верховного Суда Российской Федерации от 30 ноября 2017 года № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» // СПС «Консультант Плюс». URL: http://www.consultant.ru/document/cons_doc_LAW_283918/ (дата обращения: 15.11.2020).

[2] Приговор Братского городского суда Иркутской области от 11 января 2017 года по делу № 1-28/2017 (1-603/2016;). URL: https://bratsky--irk.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=doc&number=143609562&delo_id=1540006&new=0&text_number=1 (дата обращения: 02.12.2020).

«О судебной практике по делам о краже, грабеже и разбое», указывая, что «действия лица, совершившего незаконное изъятие имущества в отсутствие собственника или иного владельца этого имущества, следует квалифицировать как тайное хищение чужого имущества (кража), следовательно, в данном случае никакого вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации нет»; то есть Афонин лишь тайно использовал уже установленную на мобильный телефон его владельцем программу с целью незаконного обогащения[1]. С учетом вступления в силу этого разъяснения высшей судебной инстанции, а также анализа фактических обстоятельств, по нашему мнению, адекватной квалификацией является применение п. «в» ч. 3 ст. 159.6 УК РФ, то есть произошло хищение денежных средств с банковского счета с причинением значительного ущерба потерпевшему.

Поэтому наиболее приемлемым вариантом было бы выделение данного состава преступления как особой формы хищения, ведь способ совершения мошенничества в сфере компьютерной информации существенно отличается от способа совершения традиционного мошенничества и воздействует не на эмоционально-волевую сферу потерпевшего, а на нормальное функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей и состоит в нарушении установленного процесса обработки, хранения, передачи компьютерной информации, что позволяет виновному или иному лицу незаконно завладеть чужим имуществом или приобрести право на него. Именно такую позицию занимают некоторые исследователи, в частности, А. Ю. Чупрова[2].

Подводя итог вышесказанному, следует признать, что нормы о мошенничестве, в частности, в сфере компьютерной информации, нуждаются в совершенствовании со стороны законодателя, и в более подробном толковании статьи 159.6 УК РФ высшей судебной инстанцией на основе анализа существующей судебной практики. Считаю, что в Постановлении Пленума Верховного Суда Российской Федерации от 30.11.2017 № 48 «О судебной практике по делам

[1] См.: Чугунов А. А., Власенко Е. Р. Некоторые вопросы квалификации мошенничества в сфере компьютерной информации // Вестник Московского университета МВД России. 2020. № 4. С. 145.

[2] См.: Чупрова А. Ю. Проблемы квалификации мошенничества с использованием информационных технологий // Уголовное право. 2015. № 5. С. 134.

о мошенничестве, присвоении и растрате» нужно указать, что конкретно имеется в виду под «мошенничеством» в ст. 159.6 УК РФ, так как в п. 1 Постановления уже есть разъяснения по поводу других статей (158.1, 159, 159.1, 159.2, 159.3, 159.5 УК РФ), а также изменить название самой статьи 159.6 в Уголовном кодексе или вовсе исключить данный состав из перечня разновидностей мошенничества.

Список литературы

1. Журавлева Г. В, Карпова Н. А. Мошенничество в сфере компьютерной информации: спорные вопросы теории и практики // Вестник Московского университета МВД России. 2017. № 5. С. 153–158.
2. Мусаелян М. Ф. О некоторых проблемах, связанных с введением в УК РФ специальных составов мошенничества // Российский следователь. 2016. № 10. С. 26–30.
3. Чугунов А. А., Власенко Е. Р. Некоторые вопросы квалификации мошенничества в сфере компьютерной информации // Вестник Московского университета МВД России. 2020. № 4. С. 143–147.
4. Чупрова А. Ю. Проблемы квалификации мошенничества с использованием информационных технологий // Уголовное право. 2015. № 5. С. 131–134.

В. А. Баландина

ДИСТАНЦИОННЫЕ МОШЕННИЧЕСТВА: СПОСОБЫ И МЕРЫ ПРОТИВОДЕЙСТВИЯ

Аннотация: В статье рассмотрены виды и основные способы совершения киберпреступлений, а именно дистанционных мошенничеств. Указаны меры противодействия киберпреступности на примере ст. 159.3 УК РФ и актуальные проблемы расследования данных преступлений.

Ключевые слова: киберпреступление, дистанционное мошенничество, компьютерные системы, Интернет, уголовное право.

REMOTE FRAUD: METHODS AND COUNTERMEASURES

Abstract: The article discusses the types and main methods of committing cybercrimes, namely remote fraud. Measures for countering cybercrime are indicated on the example of Article 159.3 of the Criminal Code of the Russian Federation and topical problems of investigating these crimes.

Keywords: cybercrime, remote fraud, computer system, Internet, criminal law.

В современном мире государство и человек взаимодействуют с компьютерами и телекоммуникационными системами во всех сферах.

С каждым годом количество преступлений, совершаемых в виртуальном пространстве, растет пропорционально числу пользователей компьютерных сетей. По оценкам Интерпола, темпы роста преступности, например, в глобальной сети Интернет, являются самыми быстрыми на планете[1].

Преступления информационного пространства обладают повышенной общественной опасностью, так как ущерб, причиняемый данными видами преступлений, не имеет границ, возможны огромные потери, при этом такие преступления можно совершить при минимальных затратах и недолгой подготовке. Следует отметить, что киберпреступность характеризуется высокой латентностью, в результате чего статистика правоохранительных органов не отражает достоверной картины состояния киберпреступности как на уровне государства, так и на общемировом уровне[2].

Одно из самых частых киберпреступлений – дистанционное мошенничество. Говоря о субъекте преступления данных видов преступлений, следует отметить, что такие они совершаются лицом: специализирующимся на данном виде преступлений; ранее судимым за совершение аналогичных преступлений; имеющим познания в компьютерных технологиях; владеющим методами социальной инженерии; обладающим знаниями в области информационно-телекоммуникационных технологий.

Следует заметить, что существуют обстоятельства, обязательные для выяснения при выдвижении версий о возможном преступнике, связанные с знаниями преступника способов и методов совершения данного вида преступлений, информационно-телекоммуникационных технологий, компьютерных технологий, вредоносных компьютерных программ, электронных платежных систем, методов социальной инженерии, банковского дела.

Анализируя статистику преступлений, совершаемых дистанционным путем, можно выделить основные, часто совершаемые виды:

1. Объявление о продаже либо о покупке: в первом случае мошенники – продавцы выставляют объявление о продаже какого-либо товара, жертва сама связывается с ними по объявлению,

---

[1] См.: Номоконов В. А. Глобализация информационных процессов и преступность. URL: https://www.crime-research.org/library/nomokon.htm (дата обращения: 10.02.2021).

[2] См. Овчинский В. С. Основы борьбы с киберпреступностью и кибертерроризмом. М., 2017. С. 315.

перечисляет денежные средства, товар не получает. Во втором случае – жертва выставляет объявление о продаже товара, мошенники связываются с ней, просят сообщить данные банковской карты, СМС-коды для перечисления средств, впоследствии происходит хищение денежных средств с данных счетов.

2. «Сообщения от друзей» – мошенники взламывают страницы реальных людей в социальных сетях, с данных страниц пишут родственникам и друзьям с просьбой отправить им денежные средства.
3. Звонок о несчастном случае – мошенники отправляют СМС-сообщение о страшном несчастном случае от имени друга, родственника с требованием отправить денежные средства для решения ситуации.
4. Блокировка банковской карты – звонок или сообщение о блокировке банковской карты жертвы и срочным требованием назвать реквизиты карты для ее дальнейшего использования.
5. Вирус в телефоне – мошенники оставляют на разных сайтах либо рассылают в социальных сетях «зараженную ссылку». Жертва, проходя по этой ссылке, открывает доступ к своей банковской карте.

Размещая объявления в средствах массовых информаций или на портале Интернета, вы также можете стать жертвой мошенников. Приобретая понравившийся товар либо размещая объявления о продаже в газетах на порталах Интернета, сайтах «Авито» и т. д., люди, потеряв бдительность, рассчитывая на то, что продавец пообещал снизить цену на понравившийся товар либо покупатель готов купить продаваемый им товар, предоставляют реквизиты своих банковских карт мошенникам, что категорически делать нельзя, так как воспользовавшись этим, злоумышленники производят списание денежных средств с банковских карт владельцев.

Для того чтобы достигать желаемых результатов при противодействии преступлениям данного вида, необходимо при раскрытии преступления обязательно отправлять в сотовые компании и банки запросы с просьбой предоставить следующую информацию:

- на кого зарегистрированы абонентские номера, с которых звонили потерпевшим;
- абонентские номера и адреса электронной почты, которые были указаны при регистрации;
- каким образом была осуществлена регистрация пользователя;

- IP-адреса, использованные для регистрации абонентского номера;
- IP-адреса, использованные для входа в личный кабинет, панель управления по администрированию данного абонентского номера;
- IP-адреса, использованных для осуществления звонков;
- абонентские номера, на которые шла переадресация звонков;
- статистику звонков на период времени с даты совершения преступления по дату получения запроса;
- номера счетов или банковских карт, с которых осуществляется абонентская плата за использование указанного номера;
- паспортные данные владельцев, используются ли в настоящее время или нет;
- сведения о соединениях между абонентами и абонентскими номерами с привязкой к базовым станциям;
- информацию об IMEI сотовых телефонов, в которых находились сим-карты с абонентскими номерами и с которых звонили потерпевшим за период с даты совершения преступления по дату поступления запроса.

В связи с возбуждением уголовного дела на основании ч. 4 ст. 21 УПК РФ, а также в соответствии со ст. 26 Федерального закона от 02.12.1990 № 395-1 «О банках и банковской деятельности» также в банк следует отправлять запрос с просьбой предоставить расширенную выписку о движении денежных средств по карте потерпевшего с отражением сведений о номерах банковских карт, на которые были переведены денежные средства в период с даты совершения преступления по дату поступления запроса с указанием полных сведений о владельцах банковских карт и месте снятия переведенных денежных средств с указанной карты. Очень часто органы внутренних дел долго ждут ответа на данные запросы и не получают нужную информацию в срок. За это время мошенники меняют все данные, номера, местонахождение. Таким образом, требуется обязательное сокращение сроков исполнения данных запросов путем использования следователями (дознавателями) всех возможностей УПК РФ для получения необходимой информации. В соответствии с п. 4 ст. 21 УПК РФ, следователям следует обращать внимание на то, что их требования, запросы, предъявленные в пределах их полномочий, обязательны для исполнения всеми учреждениями, предприятиями, организациями, должностными лицами и гражданами. В случае невыполнения законных требований следователя, виновное

лицо будет привлечено к административной ответственности в соответствии со ст. 17.7 КоАП РФ.

Актуальным является вопрос о создании специализированных следственных отделов и подразделений, которые будут бороться именно с киберпреступностью, штат будет состоять из профессионалов, имеющих не только юридическое образование, но и знания технической и информационной направленности. Также следует использовать практику закрепления за расследованием дел о мошенничестве общеуголовной направленности конкретных следователей, которая поможет быстрее и качественнее раскрыть дело[1].

Несмотря на то, что МВД России пытается противодействовать киберпреступлениям с помощью создания дополнительных сил и средств, повышения квалификации действующих сотрудников правоохранительных органов, существуют следующие актуальные проблемы. Во-первых, расследование дела невозможно без специалистов, обладающих знаниями в сфере информационных технологий, вычислительной техники, связи. В системе МВД слабая связь экспертно-криминалистического подразделения со следственными отделами по данному вопросу. Во-вторых, нет четкой единой методической базы, методических рекомендаций, которые будут действительно эффективны при раскрытии дистанционных мошенничеств, что естественно ведет к количественному росту преступлений в данной категории. В-третьих, способы совершения данных видов мошенничеств все время меняются, совершенствуются, на данный момент нет точной классификации самих мошенничеств, устройств, с помощью которых совершается преступление, систем отслеживания. Необходимо обобщать и анализировать данные для использования полученной информации при выработке мер противодействия и в целях предупреждения киберпреступлений[2].

Список литературы

1. Кудрявцев Р. В. Организация деятельности по раскрытию дистанционных мошенничеств // Молодой ученый. 2019. № 24 (262). С. 218–221.
2. Мерецкий Н. Е., Жердев П. А. Некоторые особенности хищений денежных средств со счетов граждан при использовании услуги «Мобильный банк» // Вестник Дальневосточного юридического института МВД России. 2017. № 3 (40). С. 140–146.

[1] См.: Кудрявцев Р. В. Организация деятельности по раскрытию дистанционных мошенничеств // Молодой ученый. 2019. № 24 (262). С. 218–221.

[2] См.: Мерецкий Н. Е., Жердев П. А. Некоторые особенности хищений денежных средств со счетов граждан при использовании услуги «Мобильный банк» // Вестник Дальневосточного юридического института МВД России. 2017. № 3 (40). С. 140–146.

3. Номоконов В. А. Глобализация информационных процессов и преступность. URL: https://www.crime-research.org/library/nomokon.htm (дата обращения: 10.02.2021).
4. Овчинский В. С. Основы борьбы с киберпреступностью и кибертерроризмом. М., 2017. 528 с.

В. Б. Киракосов

ОСОБЕННОСТИ КВАЛИФИКАЦИИ МОШЕННИЧЕСТВА, СОВЕРШЕННОГО С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕХНИЧЕСКИХ СРЕДСТВ

Аннотация: Данная статья посвящена имеющимся в теории уголовного права и судебной практике дискуссионным вопросам квалификации мошенничества с использованием платежных карт. Автором исследуются проблемы применения нормы, предусматривающей уголовную ответственность за анализируемый вид мошенничества, на основе обобщения материалов судебной практики и научных позиций специалистов в области уголовного права.

Ключевые слова: мошенничество, квалификация, киберпреступление, электронные денежные средства.

FEATURES OF THE QUALIFICATION OF FRAUD COMMITTED USING INFORMATION TECHNOLOGY

Abstract: This article is devoted to the debatable issues of qualification of fraud with the use of payment cards available in the theory of criminal law and judicial practice. The author investigates problems of applying the rule providing for criminal liability for the analyzed type of fraud, based on the generalization of materials from judicial practice and scientific positions of specialists in the field of criminal law.

Keywords: fraud, qualifications, cybercrime, electronic money.

Одна из мировых тенденций развития преступности в настоящее время – совершенствование различных форм и видов хищений, направленных на денежные средства, содержащиеся в разнообразном виде: банковские карты, электронные кошельки и иные средства платежа. Наращивание технологического прогресса и требования информационного общества породили необходимость в закреплении ответственности за совершение преступлений в рассматриваемой сфере.

Проблемы квалификации и общая характеристика состава преступления. Традиционно считается, что хищение, вне зависимости от его формы, – одно из самых распространенных преступлений. Как уже было отмечено, требования современного информационного общества

обязывают государство закрепить уголовную ответственность за преступления, связанные с использованием информационно-технических средств. А. Ю. Олимпиев и И. А. Стрельникова приводят статистику, согласно которой объем хищений с банковских карт в период с января до марта 2017 года составил 1,7 млрд рублей[1].

На практике существуют проблемы, связанные с правильной квалификацией содеянного. Большое значение имеет разграничение понятий кражи и мошенничества. Если лицо завладело денежными средствами или самой банковской картой тайно, без участия потерпевшего, то данное преступление необходимо квалифицировать как кражу. В то время как, если лицо под действием обмана, открыто, вводя потерпевшего в заблуждение, завладевает его денежными средствами, то его действия надлежит квалифицировать как мошенничество. Аналогично, если лицо придумывает схему хищения денежных средств путем обмана держателей банковских карт, рассылая СМС-сообщения и осуществляя звонки, представляясь сотрудником банка, в результате чего узнает персональные данные потерпевшего, включая CVV-код на оборотной стороне банковской карты, и получает доступ к денежным средствам, то такие действия квалифицируются по статье 159 УК РФ.

Данная точка зрения является неоднозначной в науке уголовного права. Например, Олейник Е. Н. пишет о том, что в отношении денежных средств, которые находятся на банковском счету, у лица возникает право распоряжения ими. В случае, если лицо, которое не наделено правом на распоряжение конкретными денежными средствами, совершает действия, направленные на списание денежных средств с баланса банковской карты, в результате чего правомерный собственник утрачивает «контроль» над ними, то следует говорить не о мошенничестве, а о краже[2]. Трудно согласиться с данной точкой зрения. Необходимо обратить внимание на признаки кражи. Она характеризуется тем, что действия виновного лица имеют тайный характер, то есть потерпевший не знает о том, что с баланса его банковской карты совершено списание. Субъект преступления самостоятельно изымает денежные средства,

[1] См.: Олимпиев А. Ю., Стрельникова И. А. Правовой режим и методические рекомендации по расследованию хищений, совершаемых в кредитно-банковской сфере с использованием пластиковых карт и компьютерной техники // Вестник экономической безопасности. 2019. № 3. С. 201.

[2] См.: Олейник Е. Н. Проблематика отграничения кражи имущества с банковского счета от мошенничества с использованием электронных средств платежа // Балтийский гуманитарный журнал. 2018. № 2 (23). С. 404.

вопреки воли потерпевшего. Это имеет место быть в том случае, если банковская карта была по неосторожности утеряна или украдена, а виновное лицо, завладев ей, распоряжается денежными средствами, находящимися на балансе банковской карты. Однако, как уже было сказано, если виновное лицо использует определенно разработанную схему по введению потерпевшего в заблуждение и, получая от него необходимые данные, совершает списание денежных средств с банковской карты, то его действия необходимо квалифицировать как мошенничество.

Непосредственный объект рассматриваемого состава преступления – собственность физических и юридических лиц.

Особенное значение для квалификации рассматриваемого состава является объективная сторона мошенничества, совершенного с использованием разнообразных средств телекоммуникации и связи. Общеизвестно, что главным условием для наступления уголовной ответственности является наличие причинно-следственной связи между действиями виновного лица и наступившими последствиями. В данном случае описанные в статье 159 УК РФ обман и злоупотребление доверием есть способ завладения имуществом, денежными средствами. Следовательно, для наступления уголовной ответственности за рассматриваемое преступление необходима связь между обманом и переходом имущества во владения виновного лица. Третьякова Н. С. пишет, что важным является также момент окончания преступления. Мошенничество считается оконченным с момента фактического перехода имущества, денежных средств во владение виновного лица. Помимо этого, указывается, что у виновного лица возникает и возможность пользования и распоряжения имуществом[1].

Субъектом рассматриваемого состава преступления является вменяемое лицо, достигшее возраста уголовной ответственности – 16 лет. Частью третьей рассматриваемой статьи установлен специальный субъект данного состава – лицо, занимающее служебное положение.

Субъективная сторона статьи 159 УК РФ характеризуется прямым умыслом и корыстной целью совершения преступления. В данном случае понимается, что корыстная цель – это стремление изъять, распорядиться чужим имуществом как собственным, то есть виновное лицо стремится к обогащению[2].

---

[1] См.: Третьякова Н. С. Лингвистическая характеристика понятия «мошенничество»: история и современность // Уголовное право. 2015. № 5. С. 112.

[2] См.: Силкин В. П. Проблемы разграничения мошенничества со смежными составами преступлений, совершаемых с помощью обмана и злоупотребления доверием // Проблемы экономики и юридической практики. 2017. № 6. С. 195.

Законодатель также повышает степень общественной опасности мошенничества путем закрепления квалифицирующих признаков мошенничества:

1. Совершенное группой лиц по предварительному сговору / с причинением значительного ущерба гражданину (значительность ущерба определяется его имущественным положением, но не может составлять менее 5 тыс. рублей) (ч. 2 ст. 159 УК РФ);
2. Совершенное лицом с использованием своего служебного положения / в крупном размере (более 250 тыс. рублей) (ч. 3 ст. 159 УК РФ);
3. Совершенное организованной группой (устойчивая группа, которая заранее объединена для совершения одного либо нескольких преступлений) / в особо крупном размере (более 1 млн рублей) (ч. 4 ст. 159 УК РФ);
4. Сопряженное с преднамеренным неисполнением договорных обязательств в предпринимательской сфере с причинением значительного ущерба / совершенное в крупном размере / в особо крупном размере (ч. 5, 6, 7 ст. 159 УК РФ).

Правоприменительная практика. При изучении судебной практики по делам, связанным с рассматриваемым видом мошенничества, мне хотелось бы отметить, что правоприменитель также не всегда правильно квалифицирует совершенные деяния. Основную проблему судебной практики в указанном направлении составляет разграничение ст. 159 УК РФ от ст. 159.3 УК РФ. Охарактеризовать проблему такого разграничения можно даже на примере одного приговора.

Балашовский районный суд Саратовской области признал виновным Кайбалиева Н. В. в совершении 19 эпизодов мошенничества. Все эпизоды структурно похожи друг на друга: обвиняемый звонит своим жертвам, представляясь ближайшим родственником, и сообщает о выдуманном происшествии. В дальнейшем Кайбалиев просит жертву перевести определенную денежную сумму, которой должно хватить для разрешения произошедшего. Аналогичным образом осужденный совершает серию преступлений, состоящую из 19 эпизодов. Однако, несмотря на полное соответствие всех эпизодов друг другу, суд квалифицирует его действия следующим образом: эпизоды № 1–7, 9, 11, 16, 17 квалифицированы по статье 159 УК РФ, а эпизоды № 8, 10, 12–15, 18, 19 квалифицированы судом по статье 159.3 УК РФ[1]. Суд использует

[1] Приговор № 1-109/2019 1-1-109/2019 от 11 июля 2019 года по делу № 1-109/2019 Балашовского районного суда Саратовской области. URL: https://sudact.ru/regular/doc/YdEp2bCpzELd/ (дата обращения: 17.01.2021).

аналогичные формулировки при мотивировке всех эпизодов, однако делает разные выводы.

Помимо указанного случая из судебной практики, мне хотелось бы привести пример организации соответствующих мероприятий и проверок, связанных с раскрытием рассматриваемого преступления.

В процессе реализации своих трудовых обязанностей общественного помощника Прокуратуры Октябрьского района г. Ростова-на-Дону совместно с непосредственным начальником, помощником прокурора, осуществлялось исполнение поручения прокуратуры области. Поручение представляло собой сверки сведений, представленных ПАО «Сбербанк», о наличии возбужденных уголовных дел либо сообщений о преступлениях по факту хищения денежных средств с банковских счетов граждан с использованием информационно-коммуникационных технологий.

ПАО «Сбербанк» предоставило список лиц, в отношении которых были совершены подозрительные списания денежных средств, либо которые заявляли в банк о мошеннических действиях в отношении них. Лично мной были осуществлены телефонные звонки с целью выяснения обстоятельств списания денежных средств. 48 лиц из 206 не подтвердили имеющиеся данные, 28 лиц из 206 подтвердили факт необоснованного списания денежных средств. Предоставленная ими информация была оформлена рапортом помощника прокурора и направлена в поднадзорное отделение полиции с целью регистрации в Книге учета сообщений о преступлениях и проведения проверки. По итогам исполнения распоряжения прокурора области в поднадзорном отделении полиции было возбуждено три уголовных дела (одно – п. «г» ч. 3 ст. 158 УК РФ, которое в дальнейшем было переквалифицировано по ст. 159 УК РФ, два – ч. 2 ст. 159 УК РФ). Остальные 25 сообщений о преступлениях были направлены в другие отделения полиции, которым подследственна территория совершения преступления. По двадцати трем из переданных сообщений в разных районах области и города были возбуждены уголовные дела по соответствующим статьям, а по двум оставшимся были вынесены постановления об отказе в возбуждении уголовного дела в связи с отсутствием состава преступления – сумма ущерба составляла 200 рублей в одном и 350 рублей в другом случае.

На основании вышеизложенного можно сделать следующие выводы:

1. Правильная квалификация мошенничества, совершенного сиспользованием информационно-телекоммуникационных средств, несмотря на использование названия состава преступления

в словосочетании, вызывает дискуссии как в научных кругах, так и в правоприменительной практике, что свидетельствует о недостаточном правовом регламентировании рассматриваемого вопроса, либо недостаточном разъяснении по применению норм о хищении.

2. Рассматриваемый вид мошенничества определенно можно отнести к системе киберпреступлений, так как виновные лица могут, находясь на большом от жертвы расстоянии, используя информационно-технические средства, осуществить свой преступный умысел и завладеть денежными средствами либо имуществом потерпевшего.
3. Такое мошенничество квалифицируется правоохранительными органами и судом по п. «г» ч. 3 ст. 158, ст. 159, ст. 159.3 УК РФ, в зависимости от конкретных обстоятельств дела. Квалификация по первому составу представляется мне неверной.
4. Основной особенностью, которая отличает мошенничество с использованием информационно-технических средств от других видов аналогичных хищений, является то, что мошенничество совершается открыто и связано с введением потерпевшего в заблуждение, вследствие чего он самостоятельно предоставляет денежные средства виновному лицу. В то время как иные виды хищения, например, кража, характеризуются тайным хищением, неизвестным для жертвы.

Список литературы

1. Олейник Е. Н. Проблематика отграничения кражи имущества с банковского счета от мошенничества с использованием электронных средств платежа // Балтийский гуманитарный журнал. 2018. № 2 (23). С. 403–406.
2. Олимпиев А. Ю., Стрельникова И. А. Правовой режим и методические рекомендации по расследованию хищений, совершаемых в кредитно-банковской сфере с использованием пластиковых карт и компьютерной техники // Вестник экономической безопасности. 2019. № 3. С. 200–206.
3. Силкин В. П. Проблемы разграничения мошенничества со смежными составами преступлений, совершаемых с помощью обмана и злоупотребления доверием // Проблемы экономики и юридической практики. 2017. № 6. С. 195–197.
4. Третьякова Н. С. Лингвистическая характеристика понятия «мошенничество»: история и современность // Уголовное право. 2015. № 5. С. 109–112.

К. А. Ковтун

БАНКОВСКАЯ КИБЕРПРЕСТУПНОСТЬ КАК ОДНА ИЗ ОСНОВНЫХ ПРОБЛЕМ СОВРЕМЕННОГО ОБЩЕСТВА

Аннотация: В данной статье проводится изучение специфики банковских киберпреступлений, их жертв, а также преступников, совершающих данные преступления. Методом исследования является рассмотрение статистических данных Банка России. В работе автор приходит к выводу, что повышение экономической и юридической грамотности населения является наиболее эффективным способом снижения тенденции банковской киберпреступности.

Ключевые слова: экономическая безграмотность, психологическое влияние, хищения, способы предотвращения, предотвращение махинаций, способы реализации.

BANKING CYBERCRIME AS ONE OF THE MAIN PROBLEMS OF MODERN SOCIETY

Abstract: This article examines the specifics of banking cybercrimes, their victims, as well as criminals who commit these crimes. The research method is based on statistical data from the Bank of Russia. The author concludes that improving the economic and legal literacy of the population is the most effective way to reduce the trend of banking cybercrime.

Keywords: economic illiteracy, psychological influence, theft, prevention methods, fraud prevention, implementation methods.

Киберпреступность – одно из основных направлений преступности, которое набирает обороты. Преимущественный рост киберпреступлений наблюдается в XXI веке вместе с повсеместным внедрением компьютерных технологий в жизнь общества. Данный вид преступности отличается от остальных тем, что обычно целью злоумышленников становятся крупные, а не какие-то небольшие суммы, которые чаще всего наблюдаются в большинстве преступлений по статье «кража»; в киберпреступлениях, специализация которых хищение денежных средств, оборот обычно начинается с нескольких сотен тысяч и может достигать миллиардов рублей. Такие суммы связаны в первую очередь с тем, что лицо, совершающее преступление, обычно тщательно выбирает жертву, отталкиваясь от ее заработка[1].

От махинаций, связанных с хищением денежных средств со счетов, не застрахован почти никто. В истории уголовных дел встречаются случаи, когда сами сотрудники известных банков передавали информацию

[1] См.: Гамза В. А., Ткачук И. Б. Безопасность коммерческого банка: учебно-практическое пособие. М.: Издатель Шумилова И. И., 2000.

о владельце банковской карты, его паспортные данные и остальной список информации, необходимый для совершения перевода денежных средств на счет мошенника. Существует определенная схема, по которой работают мошенники, специализирующиеся на хищении средств с карт потерпевших. Сотрудник банка, имеющий отношение к данной схеме, определяет клиента, который уже долгое время не использовал свою банковскую карту, но имеет на счету банка определенное количество средств[1]. Данный сотрудник передает паспортные данные, личную информацию о содержании банковской карты мошеннику, получая за это средства. Мошенник же, проведя махинации с паспортными данными и картой, а также заверив у задействованного в схеме нотариуса, нотариально заверяет возможность снятия денежных средств с карты потерпевшего сторонним лицом, то есть оформляет доверенность. Далее, происходит хищение денежных средств со счета. Доказать, а тем более вернуть денежные средства, хищение которых произведено по данной схеме, является практически невозможным.

Банковская киберпреступность – стремительно развивающаяся отрасль. Для того чтобы похитить средства с банковского счета потерпевшего, не обязательно даже иметь какое-либо отношение к этому банку[2]. На данный момент особое развитие получила мошенническая схема, с помощью которой, по данным Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере, с банковских счетов россиян за 2020 год было похищено более пяти миллиардов рублей.

Основной причиной столь огромной цифры является финансовая и юридическая неграмотность населения. Два этих факта можно подтвердить, исходя из пояснения данной мошеннической схемы: на номер абонента поступает звонок, якобы от сотрудника известного банка, который задает простой вопрос: «Были ли совершены Вами переводы в размере нескольких тысяч рублей за ближайший час?». На что жертва отвечает, что таких транзакций не совершалось. Далее, со стороны якобы сотрудника банка начинает происходить моральное давление на абонента, которое выражается в спешке и заверении клиента в том, что если прямо сейчас тот не сообщит номер карты и секретный номер на обратной стороне, то оставшаяся сумма, находящаяся на счету абонента,

[1] Криминальная экономика и экономическая преступность. URL: www.newasp.omskreg.ru (дата обращения: 10.02.2021).

[2] См.: Сатуев Р. С., Шраер Д. Я., Яськова Н. Ю. Экономическая преступность в финансово-кредитной системе. М.: Центр экономики и маркетинга, 2000.

будет снята непосредственно этими же мошенниками. Жертва, находясь под сильным влиянием, называет все то, что от нее требуют. Исход данной махинации более чем известен.

Чем же обуславливается такое огромное количество средств, украденных мошенниками, которое исчисляется миллиардами?

Во-первых, это неграмотность, чаще всего финансовая. К примеру, пользователи Сбербанка знают, что официальный представитель банка не будет звонить абонентам с обычного номера, так как для предотвращения киберпреступлений у данного банка действует всеобщий номер телефона[1].

Во-вторых, люди, которые сильнее других подвержены психологическому влиянию, чаще попадаются в уловки мошенников. Последние же, в свою очередь, очень тщательно обдумывают ход событий, уделяя особое внимание деталям. Например, даже звук на фоне звонка мошенников полностью скопирован с бурной работы банка – на фоне слышны голоса работников Call-центра.

Вопрос, волнующий всех пострадавших од данной финансовой махинации, кто же те самые киберпреступники, которые так умело могут выводить со счетов жертв миллиарды рублей. Ответ на этот вопрос является весьма нетривиальным. Заключенные тюрем – это те, с номеров которых чаще всего совершаются звонки. Данная информация изложена в статье Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (ФинЦЕРТ) Банка России[2]. При обыске одного из московских мест отбывания наказания в камерах заключенных были найдены телефоны, роутеры, зарядные устройства, наушники, а так же блокноты с именами последующих жертв. Исходя из вышеизложенного, стоит сделать вывод, что начальство тюрьмы имеет хотя бы косвенное отношение к осуществлению мошеннических звонков. Прокуратура Российской Федерации предложила выделить средства в размере 10 млн рублей на установление приборов, способных заглушить телефонную связь на территории тюрем. Безусловно, это является одним из наиболее эффективных способов решения проблемы киберпреступности на территории тюрем.

Самым сложным и практически невозможным аспектом из данной сложившейся ситуации является возмещение ущерба клиентам банка.

---

[1] См.: Большой экономический словарь / Под ред. А. Н. Азриляна. 4-е изд. доп. и перераб. М.: Институт новой экономики, 1999.

[2] См.: Аврех Г. Наши мошенники ворочают уже биллионами // «ЗР», «ДелРосинформ». 2001. URL: www.zrpress.ru (дата обращения: 10.02.2021).

Юридически абоненты сами добровольно передавали личную информацию своих карт киберпреступникам, из-за чего возмещение денежных средств становится еще более сложным. Из всего объема похищенных средств банки возместили клиентам лишь 15 %, или 932 млн рублей. Масштаб проблемы колоссальный, способов ее решения практически нет – все это неутешительная статистика экспертов-экономистов[1].

В заключении стоит отметить, что человеческая невнимательность и неграмотность способствуют увеличению числа похищенных средств. Для уменьшения количества преступлений в данной сфере стоит предпринять меры по повышению финансовой грамотности населения, а также оповещению о наличии данной проблемы старшего поколения, которое больше остальных подвержено психологическому влиянию со стороны киберпреступников[2]. Только при совместном содействии экспертов и населения нашей стране удастся справиться с такой глобальной проблемой, как киберпреступность в банковской сфере.

Исходя из содержания главы 28 УК РФ «Преступления в сфере компьютерной информации», которая не располагает нормами регулирования киберпреступности в банковской сфере, уголовный закон не содержит нормы права, нацеленные на предотвращение махинаций с банковскими счетами. Преступления, совершаемые в данной сфере, чаще всего относят к ст. 159.6 («Мошенничество в сфере компьютерной информации»), максимальное наказание в которой составляет полтора года лишения свободы.

Резюмируем. На данный момент в УК РФ не существует статьи, которая бы была направлена на урегулирование конкретных правонарушений в сфере хищения денежных средств с банковских карт путем представления сотрудником банка и распоряжения ложной информацией. Единственным способом снижения тенденции развития преступлений в данной сфере является внесение норм права, охватывающих данную проблему. Принятие в УК РФ новой статьи в сфере киберпреступности является единственной мерой, которая способна привести к ликвидации банковской киберпреступности.

Список литературы

1. Аврех Г. Наши мошенники ворочают уже биллионами // «ЗР», «ДелРос-информ». 2001. URL: www.zrpress.ru (дата обращения: 10.02.2021).

[1] Экономическая преступность в финансово-кредитной системе России. URL: www.newasp.omskreg.ru (дата обращения: 10.02.2021).

[2] См.: Кривенко Т., Куранова Э. Расследование преступлений в кредитно-финансовой сфере. URL: www.jurga.hut.ru (дата обращения: 10.02.2021).

2. Большой экономический словарь / Под ред. А. Н. Азриляна. 4-е изд. доп. и перераб. М.: Институт новой экономики, 1999.
3. Гамза В. А., Ткачук И. Б. Безопасность коммерческого банка: учебно-практическое пособие. М.: Издатель Шумилова И. И., 2000.
4. Кривенко Т., Куранова Э. Расследование преступлений в кредитно-финансовой сфере. URL: www.jurga.hut.ru (дата обращения: 10.02.2021).
5. Криминальная экономика и экономическая преступность. URL: www.newasp.omskreg.ru (дата обращения: 10.02.2021).
6. Сатуев Р. С., Шраер Д. Я., Яськова Н. Ю. Экономическая преступность в финансово-кредитной системе. М.: Центр экономики и маркетинга, 2000.
7. Экономическая преступность в финансово-кредитной системе России. URL: www.newasp.omskreg.ru (дата обращения: 10.02.2021).

К. А. Иващенко

ЦИФРОВЫЕ КАРТЕЛИ КАК НОВАЯ РАЗНОВИДНОСТЬ КИБЕРПРЕСТУПЛЕНИЙ

Аннотация: В статье рассматриваются преступления с использованием цифровых технологий как наиболее развивающаяся разновидность преступной деятельности. В наибольшей степени это относится к преступлениям в сфере экономической деятельности, что обусловлено повсеместной цифровизацией экономических процессов в нашей стране. Особого внимания требует рассмотрение цифровой трансформации картельных сговоров, повышающей уровень латентности и общественной опасности данного преступления. На сегодняшний день остаются некоторые пробелы в законодательстве в части регламентации ответственности за преступления с использованием цифровых технологий, которые требуют глубокого осмысления.

Ключевые слова: картели, сговоры на торгах, ограничение конкуренции, цифровая преступность, киберпреступность.

DIGITAL CARTELS AS A NEW KIND OF CYBERCRIME

Abstract: The author explores crimes using digital technologies can be attributed to one of the most developing types of criminal activity, the basis of which is their commission in a virtual environment, which forms a fundamentally new content of crime. This applies to the greatest extent to crimes in the field of economic activity, which is due to the widespread digitalization of economic processes in our country. Consideration of the digital transformation of cartels, which increases the level of latency and social danger of this crime, requires special attention. There are some gaps in the legislation regarding the regulation of liability for crimes using digital technologies, which require deep understanding.

Keywords: cartels, bid rigging, restricting competition, digital crimes, cybercrime.

Развитие кибертехнологий привело как к появлению собственно цифровой экономики, так и развитию иных цифровых технологий, используемых в экономической сфере. Существенно расширив возможности по товарно-денежному обороту, совершению сделок и иным общественным отношениям в экономической сфере, цифровые технологии создали новые условия для совершения преступлений в сфере экономики. В связи с этим конкуренция между хозяйствующими субъектами становится все более интенсивной, принимает новые формы, весьма быстро влияющие на структурные изменения в экономике. Появляются новые «цифровые» рынки и цифровые инструменты, воздействующие на функционирование уже имеющихся рынков.

Происходящие трансформации также относятся и к картелям, как самым общественно-опасным нарушениям антимонопольного законодательства, которые основываются на результатах анализа больших данных, установлении и поддержании цен путем сговора посредством использования ценовых алгоритмов, аукционных роботов и иных результатов цифровой трансформации общества.

Этим обуславливается необходимость поиска новых и развития имеющихся инструментов антимонопольного регулирования, способных эффективно соответствовать практикам нового времени.

Волна цифровой трансформации деятельности картелей началась с процесса внедрения электронных торгов. Первое антимонопольное дело по сговору на электронных торгах для государственных и муниципальных нужд было возбуждено еще в 2011 году[1]. С тех пор технологии, используемые картелями, шагнули далеко вперед, и сегодня в число уже привычных для регулятора практик можно отнести использование картелями ценовых алгоритмов, аукционных роботов, систем управления проектами и иного программного обеспечения.

Согласно оценкам начальника управления по борьбе с картелями ФАС России А. П. Тенишева, в настоящее время 90 % российских картелей являются «традиционными», а 10 % – «современными» (использующими инновационные технологии), причем доля последних постоянно растет[2].

[1] См.: Тесленко А. В., Кониева Ф. И. «Роботизация» торгов – новый вызов в борьбе с картелями? // Актуальные вопросы современного конкурентного права: сборник научных трудов. Вып. 3 / Отв. ред. М. А. Егорова. М.: Юстицинформ, 2019. С. 112–122.

[2] Картель не пройдет. ФАС настаивает на усилении ответственности за антиконкурентные соглашения. URL: http://www.moskowtorgi.ru/news/Antimonopolnyy_komitet/6031 (дата обращения: 10.01.2021).

Ежедневно появляются новые цифровые инструменты в руках недобросовестных участников рынка, но некоторые из них уже плотно укоренились в практике антимонопольных органов и требуют отдельного рассмотрения.

Одним из примеров цифровых инструментов картелей являются так называемые «аукционные роботы». По сути своей «аукционный робот» представляет собой программный модуль, автоматизирующий процесс подачи ценовых предложений в ходе торгов на электронной торговой площадке в установленных ценовых пределах.

Стоит отметить, что ряд электронных торговых площадок имеет встроенный функционал «аукционного робота» на самой площадке. Наряду с ними также используются отдельные программы, обладающие соответствующим функционалом, некоторые из которых изначально созданы разработчиками для реализации антиконкурентных практик. Например, обнаруженный ФАС России аукционный робот Auctiospiner (AuSe), в описании которого на сайте разработчика указывалось, что робот может быть использован для реализации схемы «таран», а также для заметания следов при использовании прокси-серверов[1].

Очевидно, что подобные функции закладываются разработчиком в программное обеспечение исключительно с противоправной целью, а само программное обеспечение стоит особого внимания со стороны контролирующих органов.

Все чаще участники цифровых рынков прибегают к анализу больших данных (big data) в целях манипулирования ценой. Сами по себе большие данные становятся важнейшим корпоративным активом, который при определенном использовании обеспечивает их владельцам интеллектуальное превосходство и деловое доминирование на рынке. Таким образом, данные и информация становятся инструментом концентрации рыночной власти.

Справедливости ради стоит отметить, что возможности «больших данных» на сегодняшний день также используются в качестве государственного инструмента, например, при осуществлении скрининга товарных рынков и поиска картелей[2].

---

[1] См.: Антимонопольное регулирование в цифровую эпоху. Как защитить конкуренцию в условиях глобализации и четвертой промышленной революции. 2-е изд., исправл. и доп. / Под ред. А. Ю. Цариковского, А. Ю. Иванова, Е. А. Войниканис. М.: Изд. дом ВШЭ, 2019. С. 187–188.

[2] Большой цифровой кот. Промежуточные итоги и перспективы. URL: https://ilns.ranepa.ru/files/konferentsii/bolshoy-tsifrovoy-kot.pdf (дата обращения: 12.01.2021).

В числе цифровых инструментов в руках картельщиков встречаются и ценовые алгоритмы, которые представляют собой программное обеспечение, автоматически устанавливающее цены, реагируя на различные изменения: количества товаров на складе, цен конкурентов, потребительских предпочтений.

Принимая во внимание то, что системы ценового анализа становятся все более автоматизированными, одновременно с традиционной перепиской, телефонными переговорами между участниками картеля в целях установления / фиксирования цен используются компьютерные программы.

Большая часть ценовых алгоритмов относится к допустимым антимонопольным органом практикам. Вместе с тем среди них имеются отдельные виды, способствующие заключению вертикальных соглашений, картельных сговоров, координации экономической деятельности.

К числу подобных алгоритмов относится программное обеспечение, использованное российским подразделением компании LG при установлении цен на рынке смартфонов, которое было признано ФАС России антиконкурентной практикой по координации экономической деятельности[1].

Нужно отметить, что применение компьютерных программ в целях мониторинга цен на рынке не возбраняется, в то же время использование их для влияния на состояние рынка запрещено.

Экспертными советами при ФАС России по развитию конкуренции в области информационных технологий и развитию конкуренции в сфере розничной торговли в 2019 году были представлены рекомендации «О практиках в сфере использования информационных технологий в торговле, в том числе связанных с использованием ценовых алгоритмов»[2], которые также отметили недопустимость использования ценовых алгоритмов в антиконкурентных целях, одновременно представив примеры допустимых практик.

В этой связи нужно отметить, что использование аукционных роботов и иного программного продукта не может расцениваться само по себе в качестве антиконкурентного поведения, однако может являться

[1] Решение № АЦ/14552/18; Решение по делу № 1-11-18/00-22-17 от 2 марта 2018 года URL: https://br.fas.gov.ru/ca/upravlenie-po-borbe-s-kartelyami/ats-14552-18 (дата обращения: 10.01.2021).

[2] Рекомендации «О практиках в сфере использования информационных технологий в торговле, в том числе связанных с использованием ценовых алгоритмов». URL: https://fas.gov.ru/documents/684828 (дата обращени: 12.01.2021).

инструментом ограничения конкуренции в руках недобросовестных участников товарного рынка.

В научных кругах также высказывается мнение относительно необходимости введения контроля за оборотом соответствующего программного обеспечения, которое заведомо является вредоносным для конкуренции[1]. Данная позиция видится нам весьма обоснованной, поскольку создание и распространение заведомо вредоносного программного обеспечения должно квалифицироваться не как средство, а как нарушение само по себе. Не только заказчик, но и разработчик соответствующего программного обеспечения должен понимать потенциальную общественную опасность создаваемого цифрового продукта.

Актуальным также остается обсуждение положительного и негативного эффекта цифровизации в контексте антимонопольного регулирования. С одной стороны, новые механизмы реализации сговоров усложняют работу контролирующих и правоохранительных органов в части доказывания антиконкурентной направленности действий участников рынка. С другой стороны, облегчает процесс сбора и фиксации цифровых доказательств, оставляя множество следов. На сегодняшний день практически все бизнес-процессы оцифрованы, что обуславливает их большую прозрачность для контролирующих органов.

В заключение резюмируем. Несомненно, цифровизация имеет ряд положительных характеристик и должна рассматриваться как достижение общества. Вместе с тем быстрые изменения привносят определенные риски, в связи с чем задачей антимонопольных и правоохранительных органов являются своевременная реакция на новые вызовы, а также правильная правовая квалификация недобросовестных цифровых посягательств на интересы конкуренции.

Список литературы

1. Антимонопольное регулирование в цифровую эпоху. Как защитить конкуренцию в условиях глобализации и четвертой промышленной революции. 2-е изд., исправл. и доп. / Под ред. А. Ю. Цариковского, А. Ю. Иванова, Е. А. Войниканис. М.: Изд. дом ВШЭ, 2019. 394 с.
2. Тесленко А. В., Кониева Ф. И. «Роботизация» торгов – новый вызов в борьбе с картелями? // Актуальные вопросы современного конкурентного права: сборник научных трудов. Московское отделение ассоциации юристов России. Комиссия по совершенствованию антимонопольного законодательства. Вып. 3 / Отв. ред. М. А. Егорова. М.: Юстицинформ, 2019. С. 112–122.

[1] См.: Антимонопольное регулирование в цифровую эпоху... С. 341–343.

В. В. Задера

ПРОЯВЛЕНИЕ КИБЕРПРЕСТУПНОСТИ НА ИГРОВЫХ ОНЛАЙН-ПЛАТФОРМАХ: ПУТИ ЗАКОНОДАТЕЛЬНОГО РЕШЕНИЯ

Аннотация: В данной работе автором приводится дефиниция понятия киберпреступления, выделяется отдельная его разновидность – преступления, совершенные на игровых онлайн-платформах. Обращаясь к практике, автор приводит конкретные случаи игровых киберпреступлений и на их основании предлагает законодательные пути решения проблемы борьбы с киберпреступностью.

*Ключевые слова***:** киберпреступление, игровые онлайн-платформы, социальные сети, опасные вредоносные программы, мошенничество.

THE MANIFESTATION OF CYBERCRIME ON ONLINE GAMING PLATFORMS: WAYS OF LEGISLATIVE SOLUTION

Abstract: In this article the author provides a definition of the concept of cybercrime, highlights its separate type – crimes committed on online gaming platforms. Turning to practice, the author cites specific cases of gaming cybercrimes, and on their basis proposes legislative ways to solve the problem of combating cybercrime.

Keywords: cybercrime, online gaming platforms, social networks, dangerous malware, fraud.

С приходом XXI века наступило и время цифровой эпохи. На сегодняшний день цифровизация достигла всех сфер жизнедеятельности человека и общества, сейчас трудно представить обычную жизнь, работу и отдых без электронных технологий. В этом направлении развивается и наше современное государство, особенно в период пандемии COVID-19, когда многим сотрудникам пришлось перейти на систему удаленной работы. В связи с этим резко выросло количество преступлений, совершенных при помощи компьютерных технических средств и устройств, в том числе в глобальной сети Интернет и на различных игровых онлайн-платформах.

Понятие киберпреступности и киберпреступлений не новы для уголовно-правовой науки, однако, на наш взгляд, более полное и точное определение киберпреступления представляется Д. Н. Карповой, которая определяет, что киберпреступление – это акт социальной девиации с целью нанесения экономического, политического, морального, идеологического, культурного и других видов ущерба

индивиду, организации или государству с помощью любого технического средства с доступом в Интернет[1].

В понятии «киберпреступление», по нашему мнению, необходимо выделить разновидность преступлений, которые совершены с использованием компьютерных средств, технологий и устройств, направленных на охраняемые законом общественные отношения в сфере безопасного создания, обработки и хранения личной информации на игровых онлайн-платформах и средах.

Онлайн-игры – один из разновидностей досуга, который давно стал очень прибыльным делом, строящимся на продаже платных подписок и разнообразных онлайн-предметов в самих играх. Растет и монетизация игрового проекта, что в свою очередь привлекает многих киберпреступников. В целях увеличения производительности персонального компьютера во время онлайн-игры игроки отключают антивирусную защиту, тем самым сильно снижая безопасность своего устройства. В связи с этим перед онлайн-игроками появляются следующие угрозы:

1. Фишинг – преступник порождает поддельные игровые сайты. Некоторые из них используют URL-адреса, очень похожие на адреса реальных сайтов. Жертве здесь угрожают не только вредоносные программы, но и специальные ловушки, способные похитить не только личные данные, но и даже финансовые средства;
2. Социальные сети – в них работает множество мошенников с поддельными учетными записями, которые выдают себя за создателей и администраторов игровых серверов, если доверить им личные данные, то они непременно будут похищены;
3. Зараженные вирусом игры и программы – заразить свой компьютер и потерять личные данные можно через взломанные или поддельные компьютерные игры, которые мошенники предлагают загрузить через Интернет в свободном доступе;
4. Опасные вредоносные программы – в настоящее время существует ряд опасных программ, которые направлены на пользователей компьютерных игр. Эти программы способны шпионить за вводом текста с клавиатуры и могут собирать информацию, относящуюся к онлайн-играм и учетным данным пользователей[2].

---

[1] См.: Карпова Д. Н. Киберпреступность: глобальная проблема и ее решение // Власть. 2014. № 8. С. 32.

[2] См.: Номоконов В. А. Киберпреступность как новая криминальная угроза // Криминология. Вчера. Сегодня. Завтра. 2012. № 1 (24). С. 47.

Первое громкое киберпреступление произошло в 1989 году, когда неизвестные хакеры смогли запустить в компьютерную сеть американской космической программы NASA вредоносную программу «сетевого червя WANK», из-за чего пришлось отложить запуск нескольких спутников на неопределенное время. Компьютерные преступники остались без наказания.

В наше время лидером по числу киберпреступлений является World of Tanks – клиентская массовая многопользовательская онлайн-игра в реальном времени в жанре аркадного танкового симулятора. Первый случай киберпреступления на данной игровой онлайн-платформе был зафиксирован в 2012 году, в результате которого пострадавшим оказался житель г. Гомеля Республики Беларусь. У потерпевшего украли игровой аккаунт, на который, по его словам, он потратил «огромную сумму». Все закончилось благополучно, следователи вернули игровой аккаунт спустя несколько недель, мошенником оказался житель Московской области. В феврале 2016 года 36-летний военнослужащий из г. Владивостока обратился в правоохранительные органы с заявлением о пропаже виртуального танка в игре. Мошенники с помощью обмана смогли получить доступ к его электронной почте и игровому аккаунту. В короткое время местные следователи смогли отыскать пропажу, злоумышленник также остался без наказания. Также в 2016 году жители Нижегородской области из отчета о раскрываемости преступлений заместителя начальника уголовного розыска узнали о раскрытии дела «о похищении танка в World of Tanks». Гражданин приобрел игровой аккаунт в игре на сумму 70 тыс. рублей, но вскоре он был у него похищен. Мошенников смогли вычислить по IP-адресу при попытке перепродать краденный аккаунт. В ходе следственных мероприятий оказалось, что злоумышленники уже осуществляли и ранее подобные преступления. О судебном разбирательстве и мере наказания для виртуального вора не сообщалось. Эти громкие преступления были совершены только на одной игровой онлайн-платформе.

Российское уголовное законодательство предусматривает ответственность как за совершение преступлений против информационной безопасности (например, ст. ст. 272, 273 УК РФ), так и за мошенничество с использованием компьютерной информации (ст. 159.6 УК РФ), однако нет четкого алгоритма предупреждения совершения преступлений на игровых онлайн-платформах и средах. В этой связи необходимо сформулировать и предложить способы решения данной проблемы.

1. Создать и организовать постоянный контроль за ситуацией в игровой онлайн-сфере, в которой могут возникнуть угрозы

роста киберпреступности, объединить усилия широкой общественности, профессионалов, ученых и представителей органов власти для надежной защиты личных информационных ресурсов, которые будут обрабатываться и сохраняться на игровых онлайн-платформах.

2. В подразделении Министерства внутренних дел России Управлению «К», которое борется с преступлениями в сфере информационных технологий, выделить специализированный отдел, который будет расследовать преступления, совершенные только на игровых онлайн-платформах. Это приведет к снятию дополнительной нагрузки на Управление «К» и более оперативному расследованию игровых преступлений. Такие отделы необходимо ввести в территориальных органах внутренних дел.
3. Проводить активные проекты по укреплению международного сотрудничества, усовершенствованию модельного законодательства в игровой онлайн-сфере. Наладить формирование и развитие связей между органами, которые занимаются обеспечением информационной безопасности и устранением последствий угроз на игровых онлайн-платформах.

Таким образом, мы убедились, что одна из разновидностей киберпреступлений – преступления на игровых онлайн-платформах, играх и средах являются общественно-опасными деяниями, с которыми необходимо бороться. Иногда совершение даже не очень серьезного преступления может привести к опасным последствиям, которые быть могут и непоправимыми. Законодателю следовало бы принять меры по ужесточению санкций за совершение отдельных составов преступлений, имеющих отношение к данной разновидности киберпреступлений.

Список литературы

1. Карпова Д. Н. Киберпреступность: глобальная проблема и ее решение // Власть. 2014. № 8. С. 46–50.
2. Номоконов В. А. Киберпреступность как новая криминальная угроза // Криминология. Вчера. Сегодня. Завтра. 2012. № 1 (24). С. 47–52.

И. В. Мазинская

КИБЕРСТАЛКИНГ КАК НОВЫЙ ВИД ПРЕСТУПЛЕНИЯ

Аннотация: В статье рассматриваются различные подходы к определению понятия кибersталкинг, а также анализируется опыт зарубежных государств по криминализации данного деяния. Делается вывод об общественно опасном характере кибersталкинга и обосновывается необходимость введения уголовной ответственности за кибersталкинг в России.

Ключевые слова: кибersталкинг, сталкинг, киберпреступность, киберхарассмент, харассмент.

CYBERSTALKING AS A NEW TYPE OF CRIME

Abstract: The article analyzes the current procedure for the first stage of cassation proceedings in the Russian criminal process. The historical reason for the existing order of cassation appeal is revealed, its inherent problems are revealed, and the main possible ways of resolving these problems are proposed.

Keywords: cyberstalking, stalking, cybercrime, cyber harassment, harassment.

С появлением и распространением сети Интернет преступники используют новые средства для совершения преступления. Такие традиционные противоправные деяния, как кражи, вымогательства, распространение порнографии зачастую сегодня совершаются посредством сети Интернет. Национальные границы, служившие ранее ограничением для офлайн-преступлений, не имеют значения во Всемирной паутине. Это также относится к деяниям, которые с недавних пор стали признаваться мировым сообществом уголовно-наказуемыми, в том числе и к сталкингу.

Интернет используется для угроз, преследований, запугивания и домогательств. Подобное поведение принято называть кибермоббингом. Одной из форм кибермоббинга, заслуживающей особого внимания, является кибersталкинг[1].

В переводе на русский язык to stalk означает преследовать, stalker – преследователь[2].

Кибersталкеры, как и обычные сталкеры, совершают противоправные действия прежде всего с целью – запугать и причинить дискомфорт

[1] См.: Willard N. E. From Cyberbullying and Cyberthreats: responding to the challenge of online social aggression, threats, and distress. Champaign, IL: Research Press, 2007. P. 1–2.

[2] См.: Байков В. Д. Англо-русский русско-английский словарь: 45 000 слов и словосочетаний. М., 2013. С. 367.

лицу. В тоже время можно выделить существенные различия в том, как именно сталкеры достигают свои цели.

Анализ литературы и нормативно-правовых актов показывает, что дать определение кибersталкингу так же непросто, как и офлайн-сталкингу. Осложняющим фактором является отсутствие у специалистов единого мнения о том, следует ли рассматривать кибersталкинг как способ офлайн-преследования или как совершенно новый вид самостоятельного преступления, хотя и связанный с обычным сталкингом[1].

В то же время есть общее понимание того, что кибersталкинг заключается в использовании электронных информационных и коммуникационных устройств, таких как электронная почта, обмен мгновенными сообщениями, текстовые сообщения, блоги, мобильные телефоны, пейджеры, веб-сайты для запугивания или преследования конкретного лица[2].

Н. Х. Гудно выделяет пять основных различий между традиционной формой преследования и онлайн-преследованием: кибersталкеры прикладывают меньше усилий, чтобы побеспокоить своих жертв, при этом они способны распространить больший объем информации или адресовать его большему числу пользователей Сети за более короткие сроки, чем офлайн-сталкеры; могут находиться на любом расстоянии от своей жертвы; могут быть анонимными; могут выдать себя за свою жертву или использовать третьих лиц для контакта с жертвой.

На этом основании исследователь сделала вывод об уникальном характере кибersталкинга, который, по ее мнению, должен быть криминализирован в качестве самостоятельного состава преступления[3].

Следует отметить, что определенные шаги в этом направлении уже делаются. Анализ нормативно-правовых актов государств, криминализовавших сталкинг, позволяет выделить основные его признаки и сформулировать самостоятельное определение. Сталкинг – это система действий, направленных на установление контакта с конкретным лицом, нежелающим этого, совершенных с целью запугать лицо и причинить ему дискомфорт, в результате которых преследуемое лицо испытывает чувство тревоги и страха.

---

[1] См.: Kobets, P., Krasnova, K. Cyberstalking: Public danger, key factors and prevention, Przeglad Wschodnioeuropejsk. 2018. 9 (2). P. 43–53.

[2] См.: Nelufa A. Cyberstalking: a content analysis of gender-based offenses committed online. University of KwaZulu-Natal, Howard College, 2019. P. 18.

[3] См.: Goodno N. H. CS, a new crime: Evaluating the effectiveness of current state and federal laws. Missouri Law Review, 72. 2007. P. 127–132.

Соединенные Штаты Америки – первая страна, которая осознала, что сталкинг может быть совершен с использованием сети Интернет. В 49 из 50 штатов приняты законы, устанавливающие ответственность за кибersталкинг.

В некоторых штатах законодатели осуществили это путем внесения поправок в существующие законы о традиционном сталкинге, добавив, что контакт, инициированный с использованием сети Интернет или других средств связи, также представляет собой уголовно-наказуемое преследование. При этом в данных нормативных актах отсутствует понятие кибersталкинга, хотя конкретные действия, представляющие собой онлайн-преследование, запрещены. Например, в штате Колорадо кибersталкинг может осуществляться путем отправления сообщений или оставления непристойных комментариев, просьб, предложений, направленных лицу с помощью телефона, телефонной сети, сети передачи данных, текстового сообщения, компьютерной сети или другого электронного средства связи, осуществленного в целях преследования, а также сопровождающееся угрозой причинения телесных повреждений или повреждениями имущества данному лицу[1].

Другие штаты приняли закон, содержащий определение кибersталкинга, и данное деяние выделяется ими в качестве самостоятельного состава преступления. В частности, в штате Калифорния кибersталкингом признается поведение, направленное на общение с конкретным лицом или побуждение этого лица к общению с помощью электронной почты или других электронных средств связи, вызывающее у этого лица существенные эмоциональные страдания и не служащее никакой законной цели[2].

В Уголовном кодексе Германии 1899 года понятие кибersталкинга отсутствует. При этом рассматриваемое деяние признается одним из способов совершения обычного сталкинга, под которым законодатель понимает попытку установить контакт с нежелающим этого лицом с помощью использования различных средств связи. Для привлечения кибersталкера к уголовной ответственности необходимо доказать, что потерпевший испытал чувство страха[3].

---

[1] Уголовный кодекс штата Колорадо, США 1964 г. ст. 18-9-111. URL: https://codes.findlaw.com/co/title-18-criminal-code/co-rev-st-sect-18-9-111.html (дата обращения: 10.01.2021).

[2] Уголовный кодекс штата Калифорнии, США 1872 г. ст. 422. URL: https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=PEN&heading2=TITLE%20OF%20THE%20ACT (дата обращения: 10.01.2021).

[3] Уголовный кодекс Германии 1899 г. ст. 238. URL: http://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html#p2181 (дата обращения: 10.01.2021).

В Австралии, также как и в Германии, кибersталкинг является лишь формой противоправного преследования, осуществляемого по телефону, почте, факсу, электронной почте или с использованием других технологий[1].

В Японии действия, представляющие собой кибersталкинг, были криминализированы в 2017 году. К ним относится отправка сообщения в социальных сетях и по электронной почте, написание сообщений в блогах, даже если они не были прочитаны потерпевшим. Данные действия должны иметь продолжительный, навязчивый характер и совершаться с целью удовлетворить чувство любви сталкера, вызвать расположение или негодование у жертвы[2].

Краткий анализ зарубежного уголовного законодательства позволяет сделать вывод, что кибersталкингом признается вид сталкинга, осуществляемый с помощью сети Интернет или других средств связи. При этом зарубежные государства не выделяют кибersталкинг в качестве самостоятельного состава преступления, хотя и признают его общественно опасный характер.

Кибersталкинг действительно является общественно опасным деянием. Понимание, что сталкер может получить доступ к жертве в любое время, при этом находясь на любом расстоянии от нее, вызывает у жертвы чувства страха и беспомощности, что наносит вред ее психическому здоровью. Кибersталкинг, как и обычный сталкинг, может являться предварительным этапом совершения более тяжких преступлений – причинения тяжкого вреда здоровью, изнасилований, убийств. По данным исследования, проведенного Американской психиатрической ассоциацией, 36 % сталкеров нападали на свою жертву[3].

Следует признать, что Интернет предлагает широкие возможности для использования передовых компьютерных программ, которые кибersталкер сможет применять в своих противоправных целях. Но вычислить преступника и доказать совершение им указанных действий достаточно сложно. Особенно, если преследователь осуществляет это, находясь в другом государстве.

---

[1] Уголовный кодекс штата Квинсленда, Австралия 1899 г. ст. 359B. URL: https://www.legislation.qld.gov.au/view/pdf/2019-05-07/act-1899-009 (дата обращения: 10.01.2021).

[2] Закон, вносящий изменения в Закон «О борьбе со сталкингом». -URL: http://www.shugiin.go.jp/internet/itdb_gian.nsf/html/gian/honbun/houan/g19202051.htm (дата обращения: 10.01.2021).

[3] Мюллен П. Организация помощи сталкерам // Обзор современной психиатрии. 2003. № 18. С. 102.

Официальная информация о случаях кибersталкинга на территории России пока отсутствует. Но анализ статистических данных позволяет сделать определенные прогнозы. Известно, что сегодня более 80 % российских граждан являются интернет-пользователями[1]. Это отразилось и на количестве преступлений, которые совершаются с использованием интернет-технологий. В 2020 году количество киберпреступлений в России выросло на 91,7 % по сравнению с прошлым годом[2].

Действующее уголовное законодательство предусматривает ответственность за некоторые деяния, которые может осуществлять кибersталкер, например, угрозы, клевету, доведение до самоубийства, но большинство случаев онлайн-преследования остаются вне поля зрения правоохранительных органов. Это связано с тем, что отдельные действия кибersталкера первоначально не представляют общественной опасности, но когда они приобретают систематический, назойливый характер, то способны повлечь за собой тяжкие последствия для потерпевших. С неминуемым ростом количества пользователей сети Интернет следует ожидать, что в России будет увеличиваться и число жертв, пострадавших от кибersталкинга. Именно поэтому так важно выработать законодательство, способное защитить граждан от этого общественно опасного деяния, признать данное деяние самостоятельным составом преступления.

Список литературы

1. Байков В. Д. Англо-русский русско-английский словарь: 45 000 слов и словосочетаний. М., 2013.
2. Мюллен П. Организация помощи сталкерам // Обзор современной психиатрии. 2003. № 18.
3. Goodno N. H. CS, a new crime: Evaluating the effectiveness of current state and federal laws. Missouri Law Review, 72. 2007. P. 127–132.
4. Kobets, P., Krasnova, K. Cyberstalking: Public danger, key factors and prevention, Przeglad Wschodnioeuropejsk. 2018. 9 (2). P. 43–53.
5. Nelufa A. Cyberstalking: a content analysis of gender-based offenses committed online. University of KwaZulu-Natal, Howard College, 2019.
6. Willard N. E. From Cyberbullying and Cyberthreats: responding to the challenge of online social aggression, threats, and distress. Champaign, IL: Research Press, 2007. P. 1–2.

[1] Данные опроса ВЦИОМ-Спутник о количестве интернет-пользователей. URL: https://wciom.ru/ratings/polzovanie-internetom (дата обращения: 10.01.2021).

[2] Информация МВД России о состоянии преступности в России в 1-м полугодии 2020 года. URL: https://мвд.рф/news/item/20580266 (дата обращения: 10.01.2021).

А. С. Чуманов

ПРОБЛЕМЫ ПРОТИВОДЕЙСТВИЯ НЕЗАКОННОМУ ОБОРОТУ НАРКОТИЧЕСКИХ СРЕДСТВ, ПСИХОТРОПНЫХ ВЕЩЕСТВ ИЛИ ИХ АНАЛОГОВ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ

Аннотация: В статье рассматриваются актуальные проблемы противодействия уголовно-правовыми методами незаконному обороту наркотических средств, психотропных веществ или их аналогов с использованием информационно-телекоммуникационных сетей, в частности, путем внесения изменений в уголовный закон (ст. 228 и 228.1 УК РФ).

Ключевые слова: информационно-телекоммуникационные сети, мессенджеры, киберпреступность, наркотические средства.

PROBLEMS OF COUNTERING ILLICIT TRAFFIC IN NARCOTIC DRUGS, PSYCHOTROPIC SUBSTANCES OR THEIR ANALOGUES USING INFORMATION AND TELECOMMUNICATION NETWORKS

Abstract: The article considers the current problems of countering criminal legal methods of illegal trafficking in narcotic drugs, psychotropic substances or their analogues using information and telecommunication networks, in particular, by amending the criminal law (Articles 228 and 228.1 of the Criminal Code of the Russian Federation).

Keywords: information and telecommunication networks, messengers, cybercrime, drugs.

В Указе Президента РФ от 31.12.2015 № 683 «О Стратегии национальной безопасности Российской Федерации» в разделе II п. 22 отмечено, что главной угрозой общественной безопасности является «деятельность преступных организаций и группировок, в том числе транснациональных, связанная с незаконным оборотом наркотических средств и психотропных веществ».

В настоящее время все больше с использованием информационно-телекоммуникационных сетей население вовлекается в употребление наркотических средств. Мессенджеры (Telegram, WhatsApp, Viber) значительно упрощают возможность сбыта наркотических средств без непосредственного контакта между наркодилером и покупателем.

За последние пять лет благодаря развитию сети Интернет возникло большое количество форм данной противоправной деятельности, сложились структуры сбыта наркотических средств. Данные структуры

отличаются своей конспирацией на всех этапах, начиная с момента заказа на интернет-странице или приложения, заканчивая перечислением денежных средств (чаще всего безналичным способом) и получением адреса места закладки наркотических средств[1]. При этом установить личность, как продавца, так и покупателя, в данном механизме купли-продажи затруднительно, так как все лица остаются анонимными.

Доказывание причастности к сбыту наркотических средств через социальные сети и другие интернет-ресурсы является тяжелой задачей для правоохранительных органов. Законодатель в связи с этим предусмотрел в п. «б» ч. 2 ст. 228.1 УК РФ для лиц, распространяющих наркотические средства с использованием информационно-телекоммуникационных сетей (включая сеть Интернет), более строгую ответственность вплоть до 12 лет лишения свободы.

Но перед тем, как прийти к столь суровой санкции, необходимо провести цепь доказывания. Главной проблемой при доказывании преступлений по ст. ст. 228 и 228.1 УК РФ является прежде всего установление лиц, совершивших деяние, так как информационные технологии позволяют скрывать свои личные и какие-либо данные, оставаясь анонимным пользователем.

Для начала раскроем процедуру сбыта наркотических средств через интернет-ресурсы, покажем распределение ролей в этой преступной деятельности. Начальным звеном в реализации наркотических средств является так называемый «складчик», он получает крупные партии наркотиков, хранит и фасует их на мелкооптовые партии. Конечным звеном является «закладчик», который размещает мелкие партии наркотиков в тайниках и «покупатель», который забирает данный товар.

Для обеспечения связи между «покупателем» и «закладчиком» образуется группа в рамках сообщества социальной сети. В данной группе работают следующие лица: «администратор», который разрешает споры между «покупателями» и «закладчиками», «куратор», который контролирует работу «закладчиков». Также для обеспечения набора кадров в виде «закладчиков» в группе существуют такие должности, как «менеджер по персоналу» и «оператор», они проводят анкетирование «закладчиков» и определяют их место работы[2].

[1] См.: Глушков Е. Л. Сбыт наркотических средств бесконтактным способом посредством сети Интернет: пути выявления и раскрытия // Проблемы правоохранительной деятельности. 2018. № 2. С. 48.

[2] Приговор № 1-140/2020 от 28 мая 2020 года по делу № 1-140/2020 Нерюнгринского городского суда (Республики Саха (Якутия). URL: https://sudact.ru/regular/doc/abjabQRYzUUw/ (дата обращения: 16.01.2021).

По сути, мы имеет организованную группу, определяемую в ч. 3 ст. 35 УК РФ. Участники данной группы остаются анонимными, и у правоохранителей мало средств для закрытия данных групп и мало способов для раскрытия личностей, выполняющих различные функции в вышеназванных социальных сетях, специализирующихся на сбыте наркотиков. Это обусловлено тем, что сообщества в социальных сетях, например в мессенджере «Телеграм», при блокировке IP-адреса могут получить новый[1], а для установления личностей нет достаточной информации в социальных сетях для идентификации человека.

Анализируя практику судов при разрешении дел по ст. ст. 228 и 228.1 УК РФ, можно прийти к выводу, что из данной группы чаще всего привлекаются к ответственности именно «закладчики» и «покупатели», в некоторых случаях «администраторы»[2], поскольку именно эти лица задерживаются полицейскими непосредственно при перевозке наркотических средств. Остальные участники этой организованной группы остаются неустановленными, и продолжают свою преступную деятельность.

Лишившись «закладчиков», данные организации путем рассылки по электронной почте, размещая вакансии, набирают новых людей для пересылки наркотических средств «покупателям». Соответственно, привлечение к ответственности «закладчиков» не останавливает процесс наркоторговли, остальные соучастники продолжают привлекать новых людей.

Противодействовать данному способу, как было сказано, тяжело и в большей степени это касается сферы уголовно-процессуального права, но помимо процессуальных мер можно предпринять и уголовно-правовые.

Во-первых, если п. «б» ч. 2 ст. 228.1 УК РФ предусмотрена более строгая ответственность за сбыт наркотических средств путем использования средств массовой информации либо электронных или информационно-телекоммуникационных сетей (включая сеть Интернет), то почему в ст. 228 УК РФ за приобретение наркотических средств путем использования сетей Интернет, в частности, с использованием мессенджеров, не предусмотрена более строгая ответственность.

[1] См.: Суходолов А. П., Бычкова А. М. Цифровые технологии и наркопреступность: проблемы противодействия использованию мессенджера «Телеграм» в распространении наркотиков // Всероссийский криминологический журнал. 2019. № 1. С. 13.

[2] Приговор № 1-210/2020 от 21 мая 2020 года по делу № 1-210/2020 Железнодорожного районного суда г. Барнаула (Алтайский край). URL: https://sudact.ru/regular/doc/DSsEzSQYGfa/ (дата обращения: 16.01.2021).

Необходимость введения данного способа приобретения наркотических средств основана на том, что «покупатель» совершает данное деяние с большей общественной опасностью, чем предусматривает ч. 1 ст. 228 УК РФ, так как лицо совершает преступление анонимно, поэтому правоохранительным органам трудно вычислить лицо и доказать причастность к преступлению.

Исходя из этого, в ч. 2 или 3 ст. 228 УК РФ следует добавить квалифицирующий признак «приобретение наркотических средств, психотропных веществ или их аналогов путем информационно-телекоммуникационных сетей Интернет или сервисов обмена мгновенными сообщениями», предусмотрев более строгую ответственность.

Во-вторых, следует увеличить ответственность «закладчиков», которые выполняют пересылку наркотических средств, используя при этом социальные сети. Как правило, деяние сопровождается тем, что «закладчик» предоставляет ответную информацию через сеть Интернет «куратору», который впоследствии связывается с «покупателем» и сообщает ему место хранения наркотиков. Соответственно, следует внести изменения в ч. 2 ст. 228.1 УК РФ и изложить ее следующим образом: «Сбыт или пересылка наркотических средств, психотропных веществ или их аналогов, совершенные …».

Предложенные меры смогут, на мой взгляд, существенно сократить число преступных деяний, совершаемых с использованием информационно-телекоммуникационных сетей. Эти меры будут носить превентивный характер, противодействуя совершению преступлений данной направленности.

Список литературы

1. Глушков Е. Л. Сбыт наркотических средств бесконтактным способом посредством сети Интернет: пути выявления и раскрытия // Проблемы правоохранительной деятельности. 2018. № 2. С. 45–52.
2. Суходолов А. П., Бычкова А. М. Цифровые технологии и наркопреступность: проблемы противодействия использованию мессенджера «Телеграм» в распространении наркотиков // Всероссийский криминологический журнал. 2019. № 1. С. 5–17.

М. А. Маньков

К ВОПРОСУ ОБ УГОЛОВНОЙ ОТВЕТСТВЕННОСТИ ЗА КИБЕРТЕРРОРИЗМ

Аннотация: Статья посвящена проблеме включения ответственности за кибертерроризм в уголовный закон. Анализируется и обосновывается необходимость интегрирования квалифицированного состава «кибертерроризм» в Особенную часть УК РФ.

Ключевые слова: кибертерроризм, террористический акт, кибертеракт, киберпространство, преступление.

TO THE QUESTION OF CRIMINAL LIABILITY FOR CYBERTERRORISM

Abstract: This article is devoted to the problem of including liability for cyberterrorism in criminal law. The author analyzes and substantiates the need to include a qualified corpus delicti “cyber terrorism” in the Special Part of the Criminal Code of the Russian Federation.

Keywords: cyber terrorism, terrorist act, cyber terrorist attack, cyberspace, crime.

Кибертерроризм является самой опасной и масштабной формой террористической деятельности[1]. В силу высокой зависимости современных инфраструктур от информационных систем и киберпространства, урон от кибертеракторов всегда неизбежно влечет катастрофические последствия и причиняет колоссальный вред интересам национальной безопасности государств[2]. Известны случаи, когда кибертеррористы дистанционно захватывали космические спутники, как было с британским Skynet4-D; завладевали стратегической информацией, примером чего является инцидент хищения электронных документов Пентагона Х. Ландером; парализовывали работу ядерной промышленности, как в 2010 году в Иране; устраивали глобальные кибертеракты всемирного масштаба, что произошло в 2017 году, когда вирус WannaCry нанес вред информационным ресурсам 150 стран, включая Российскую

[1] См.: Кобец П. Н., Краснова К. А. О современных информационных технологиях, используемых экстремистскими и террористическими организованными группами, и необходимости противодействия киберпреступности // Вестник Дальневосточного юридического института МВД России. 2018. № 2 (43). С. 75–79.

[2] См.: Панталева Н. С. Кибертерроризм и киберэкстремизм как современные угрозы национальной и международной безопасности // Юридическая наука. 2019. № 3. С. 47–49.

Федерацию[1]. Современной России необходимо комплексно противостоять кибертеррактам, в том числе и в правовом поле. Сейчас кибертерроризм нормативно не закреплен в актах, регулирующих сферу антитеррористической безопасности в РФ, что затрудняет возможности правового противодействия ему[2]. Для обеспечения наказуемости, предупреждения, упрощения определения и квалификации кибертеррактов представляется необходимым ввести в УК РФ квалифицированный состав, предусматривающий ответственность за кибертерроризм.

Предполагаемый уголовный состав кибернетического терроризма должен иметь как сходство с составом террористического акта, предусмотренного ст. 205 УК РФ (далее – ст. 205), так и различия. В объективной стороне он будет отличаться особенностями совершаемых преступных действий, а также дополнительными признаками преступления. При конструировании объективной стороны нужно указать, что кибертеракт осуществляется устрашающими население действиями с использованием компьютеров, информационных систем, телекоммуникационных сетей[3]. Данное уточнение отграничит действия субъектов, совершающих кибертеракт, от действий при совершении типичного террористического акта, что важно для работы механизма квалификации. Дополнительные признаки объективной стороны кибернетического террористического акта полагаем возможным определять так же, как они определяются в теории уголовного права для преступлений против компьютерной информации. Орудием следует считать компьютерную технику, оборудование и устройства; средствами – вредоносные компьютерные программы, компьютерные технологии и ИТКС; способом – совокупность противоправных действий в Сети, осуществляемых с использованием указанных программ и устройств[4].

Представляется, что субъективная сторона кибернетического террористического акта не должна отличаться от аналогичного элемента состава ст. 205. При описании цели деяния можно руководствоваться

---

[1] См.: Васильев М. Кибертерроризм как элемент глобальной войны. URL: https://www.geopolitica.ru/article/kiberterrorizm-kak-element-gibridnoy-voyny (дата обращения: 10.02.2021).

[2] См.: Диденко А. И. Понятие и место кибертерроризма в уголовном праве России // Отечественная юриспруденция. 2016. № 9 (11). С. 17–21.

[3] См.: Саломатина Е. С. Перспективы развития законодательства в сфере борьбы с кибертерроризмом // Закон и право. 2009. № 1. С. 47–48.

[4] См.: Бочкин Д. В. Способы совершения компьютерных преступлений и использование информационных технологий как способ совершения преступления // Сибирские уголовно-процессуальные и криминалистические чтения. 2016. № 5 (13).

уже имеющимися положениями состава «террористический акт», но указать, что кибертеракт наносит вред именно информационным инфраструктурам для дестабилизации обстановки в стране, оказания воздействия на принятие решений органами власти, международными организациями. Кибертерроризм стремится к тем же результатам, что и иные формы террористической угрозы. Он ставит своей задачей оказание политического влияния на обстановку в стране и мире и этим будет схож с типичным терроризмом и отличаться от стандартных преступлений против компьютерной информации, указанных в главе 28 УК РФ, не имеющих террористических целей и подразумевающих преступные мотивы корыстной или иной личной заинтересованности[1].

Субъект кибертерроризма не должен отличаться от аналогичного элемента состава преступления, предусмотренного ст. 205, – вменяемое лицо, достигшее 14 лет.

Объект и предмет претерпят некоторые изменения. Основным объектом следует определить правоотношения, охраняющие общественную безопасность, а дополнительными объектами – правоотношения, охраняющие жизнь, здоровье, имущественные или иные интересы физических или юридических лиц[2]. К числу дополнительных объектов нужно отнести также правоотношения, охраняющие компьютерную информацию, безопасность информационных систем, ведь они тоже страдают в ходе кибертеракторов. В качестве предметов кибернетического терроризма полагаем возможным представить: компьютеры, информацию, аппаратуру передачи данных, информационные системы и иные компоненты информационной структуры, так как эта форма терроризма причиняет вред государственным и в некоторых случаях частным информационным структурам[3]. Государственная система информационной инфраструктуры поддерживает функционирование всех информационных сервисов, в том числе систем, обеспечивающих деятельность критической инфраструктуры РФ[4]. Выход из строя данных объектов

---

[1] См.: Преступления в сфере компьютерной информации: учебное пособие / А. Н. Попов. СПб.: Санкт-Петербургский юридический институт (филиал) Университета прокуратуры Российской Федерации, 2018. С. 15.

[2] См.: Трунцевский Ю. В. Неправомерное воздействие на критическую информационную инфраструктуру: уголовная ответственность ее владельцев и эксплуатантов // Журнал российского права. 2019. № 5. С. 99–106.

[3] См.: Мазуров В. А. Кибертерроризм: понятие, проблемы противодействия // Доклады ТУСУРа. 2010. № 1 (21). Ч. 1. С. 41–45.

[4] Формы терроризма. URL: https://www.mrsu.ru/ru/antiterror/theory.php?ID=15255 (дата обращения: 10.02.2021).

неизбежно повлечет тяжкие последствия в виде социальных, политических, экономических и экологических кризисов, являющихся более общественно опасными, чем результаты классических террористических акций – последствия взрыва, поджога[1].

Кибернетический терроризм следует отличать от информационного терроризма. Информационный терроризм распространяет устрашающую информацию о террористической деятельности, пропагандирует идеологию терроризма, в том числе посредством информационных технологий, и может быть квалифицирован по ч. 2 ст. 205.2 УК РФ. При кибертерроризме выводятся из строя элементы информационных структур или их целостное единство, разрушается киберпространство[2]. Это также влечет устрашение, но кибертеракт отличается большей общественной опасностью (кибертерроризм непосредственно вредит информационной структуре, а не просто распространяет незаконную информацию), иными предметами преступления (объекты информационных систем, а не только информационное поле), способом и средствами его осуществления (реализация совокупности мер по выведению из строя элементов информационных структур). Кибертерроризм не закреплен в УК РФ, и мы полагаем необходимым создать специальную уголовно-правовую норму для эффективного правового противодействия кибертеррактам.

Сейчас нет консенсуса в споре о форме включения кибертерроризма в УК РФ. Существует мнение (А. И. Диденко), по которому его нужно ввести в Особенную часть в форме самостоятельного основного состава, закрепив в главе 24[3]. Ряд авторов (И. Г. Чекунов, Е. С. Соломатина, Е. А. Капитонова) считают, что кибертерроризм следует интегрировать в УК РФ путем включения квалифицирующих признаков в ст. 205 в виде дополнительных части или пункта, предусматривающих ответственность за осуществление террористического акта с использованием компьютерной техники, направленного на выведение из строя элементов информационной структуры. Есть точка зрения (Е. В. Старостина, Д. Б. Фролов, В. Н. Черкасов), согласно которой для квалификации кибертеррактов

---

[1] См.: Трунцевский Ю. В. Неправомерное воздействие на критическую информационную инфраструктуру: уголовная ответственность ее владельцев и эксплуатантов // Журнал российского права. 2019. № 5. С. 101.

[2] См.: Мазуров В. А. Кибертерроризм: понятие, проблемы противодействия // Доклады ТУСУРа. 2010. № 1 (21). Ч. 1. С. 41–45.

[3] См.: Диденко А. И. Понятие и место кибертерроризма в уголовном праве России // Отечественная юриспруденция. 2016. № 9 (11). С. 17–21.

достаточно существующего состава ст. 205. Сторонники этой идеи утверждают, что признаки кибертерроризма полностью охватываются составом преступления «террористический акт», а преступные операции с использованием компьютерной техники возможно определить, как «иные действия», указанные в диспозиции ст. 205[1].

Правильным представляется решение проблемы путем включения признаков кибернетического терроризма, как квалифицирующих в ст. 205. Кибертерроризм имеет много общего с составом террористического акта и соотносится с ним видом умысла, устрашающими население действиями, политическими целями. Вместе с этим кибертеракты будут отличаться орудиями, средствами и способами совершения, предметами посягательства, особенностями преступных действий, связанных с применением компьютерной техники, а также более опасными и глобальными последствиями в сравнении с результатами взрыва или поджога. Поэтому кибертерроризм не может стать самостоятельным основным составом, так как имеет признаки уже включенных в УК РФ деяний, что не создает необходимости перегружать кодекс новой статьей, но и не может остаться без упоминания, так как представляет из себя отдельное, более общественно опасное, в силу своей масштабности и неуязвимости, преступление, обладающее уникальными признаками и более глобальными последствиями, чем стандартные террористические акции. С мнением ученых, предлагающих отнести кибертеракты к «иным действиям», указанным в ст. 205, нельзя согласиться, так как в 2012 году Верховный Суд РФ, обобщая судебную практику по делам о преступлениях террористической направленности, конкретизировал упомянутые в статье «иные действия» и не указал среди них признаки кибертерроризма[2]. Исходя из всего выше сказанного, наиболее оптимальным видится вариант введения кибертеракта в УК РФ, как квалифицированного состава ст. 205.

Таким образом, включение кибертерроризма в УК РФ является возможным и необходимым шагом в направлении оптимизации уголовного закона для противодействия высокотехнологичным террористическим акциям. Однако данная проблема до сих пор не урегулирована и требует

---

[1] См.: Капитонова Е. А. Особенности кибертерроризма как новой разновидности террористического акта // Известия высших учебных заведений. Поволжский регион. Общественные науки. 2015. № 2 (34). С. 29–41.

[2] Постановление Пленума Верховного Суда Российской Федерации от 09.02.2012 № 1 «О некоторых вопросах судебной практики по уголовным делам о преступлениях террористической направленности» // СПС «Консультант Плюс», 2021.

решения. Одним из вариантов которого могут быть предложенные в настоящей работе изменения в Особенной части УК РФ.

Список литературы

1. Бочкин Д. В. Способы совершения компьютерных преступлений и использование информационных технологий как способ совершения преступления // Сибирские уголовно-процессуальные и криминалистические чтения. 2016. № 5 (13).
2. Васильев М. Кибертерроризм как элемент глобальной войны. URL: https://www.geopolitica.ru/article/kiberterrorizm-kak-element-gibridnoy-voyny (дата обращения: 10.02.2021).
3. Диденко А. И. Понятие и место кибертерроризма в уголовном праве России // Отечественная юриспруденция. 2016. № 9 (11). С. 17–21.
4. Капитонова Е. А. Особенности кибертерроризма как новой разновидности террористического акта // Известия высших учебных заведений. Поволжский регион. Общественные науки. 2015. № 2 (34). С. 29–41.
5. Мазуров В. А. Кибертерроризм: понятие, проблемы противодействия // Доклады ТУСУРа. 2010. № 1 (21). Ч. 1. С. 41–45.
6. Преступления в сфере компьютерной информации: учебное пособие / А. Н. Попов. СПб.: Санкт-Петербургский юридический институт (филиал) Университета прокуратуры Российской Федерации, 2018. 68 с.
7. Панталева Н. С. Кибертерроризм и киберэкстремизм как современные угрозы национальной и международной безопасности // Юридическая наука. 2019. № 3. С. 47–49.
8. Саломатина Е. С. Перспективы развития законодательства в сфере борьбы с кибертерроризмом // Закон и право. 2009. № 1. С. 47–48.
9. Трунцевский Ю. В. Неправомерное воздействие на критическую информационную инфраструктуру: уголовная ответственность ее владельцев и эксплуатантов // Журнал российского права. 2019. № 5. С. 99–106.

О. И. Бахолдин

К ВОПРОСУ О ПОНЯТИИ КИБЕРТЕРРОРИЗМА

Аннотация: В статье рассмотрено возникновение такого явления, как кибертерроризм. Выявлены основные цели, субъекты, общественная опасность данного явления, а также меры по его предотвращению в современном мире.

Ключевые слова: кибертерроризм, технологии, нормативное закрепление, противодействие терроризму.

ON THE QUESTION OF THE CONCEPT OF CYBER TERRORISM

Abstract: The article examines the emergence of such a phenomenon as “cyber terrorism”. The main goals, subjects, social danger of this phenomenon, as well as measures to prevent it in the modern world are identified.

Keywords: cyberterrorism, technologies, normative consolidation, countering terrorism.

Формирование информационных технологий определило еще один объект атак террористов, и эффективность этих атак может превзойти все ожидания. Информационная составляющая активно используется радикальными структурами и террористическими группировками в своей деятельности, являясь при этом и объектом, и средством воздействия. В настоящее время очевидно, что деятельность общественных институтов все больше зависит от использования информационных технологий, но более продуктивный способ давления на правительство – влияние на людей с помощью информационных технологий. Непосредственно по этой причине более опасные формы незаконного применения данных проявляются в терроризме: при его пропаганде и напрямую в акциях.

Такое понятие как «кибертерроризм» возникло в 1980 году. Один из исследователей Института безопасности и разведки в штате Калифорния Барри Коллин предположил, что если какая-нибудь из передовых технологий попадет в руки террористов, то это может приобрести трагические последствия. И время не заставило долго ждать, уже буквально через десять лет на одной АЭС в Литве террористы захватили компьютерный контроль над станцией с помощью «Троянского коня». Действия террористов были оперативно обезврежены, что предотвратило техногенную аварию[1].

[1] См.: Капитонова Е. А. Особенности кибертерроризма как новой разновидности террористического акта // Известия высших учебных заведений. Поволжский регион. № 2 (34). С. 33.

Таким образом, можно увидеть, что целью кибертерактов является выведение различными методами из строя информационной инфраструктуры государства, последствия которого являются катастрофическими для стран. Основными мишенями для проведения подобных актов являются страны, которые имеют в своем распоряжении высокие технологии в области спутниковой связи и глобальных сетей. Кибертеракт может быть направлен на ключевые элементы инфраструктуры любой страны, такие как:

1. Электричество: атака на системы управления через беспроводные модемы или интернет-соединения может послужить причиной временного локального отключения электропитания;
2. Транспорт: нападающий обладает вероятностью подсоединиться к системе управления железнодорожными путями, что приводит к столкновению поездов и подобным транспортным происшествиям;
3. Водные ресурсы: путем атаки на систему управления через Интернет возможно повысить содержание хлора и других химических веществ в системе подачи воды в населенные пункты, а также обесточивание очистных сооружений, что может привести к экологическим загрязнениям;
4. Энергетика: временное отключение источников энергии;
5. Финансы: возможность закрытия финансового рынка путем выведения серверов из строя, используя сетевого червя;
6. Информационные технологии: вероятность получения доступа к критичным системам благодаря уязвимости программного обеспечения, которые могут вызвать различные атаки в прочие компоненты существующей информационной системы, а так же создать расширенные проблемы со связью во Всемирной паутине[1].

В 2016 году в одном из медицинских центров Голливуда был захвачен сервер по управлению больничным компьютерами, которые обеспечивали работу аппаратов жизнеобеспечения, тем самым поставив под угрозу жизни людей, подключенных к этим аппаратам. Заблокированы были также и средства связи с внешним миром.

Работа террористов в сети Интернет, как правило, делится на три основные группы: активность, хакерство и кибертерроризм.

Под активностью стоит подразумевать простое использование компьютерных технологий. В этом случае киберпространство выступает

[1] См.: Карамова Э. И. К вопросу о кибертерроризме в глобализирующемся мире // Социально-политические науки. № 3. С. 154.

средством, содействующим объединению террористов, рекрутированию новых членов в террористические формирования.

Хакерство предполагает преступные атаки в компьютерные сети, засекреченные базы данных, а также веб-сайты с целью извлечения той или иной выгоды или данных, либо хищения денежных средств.

Что касается кибертерроризма, то, несмотря на то, что он и схож по способам его осуществления с хакерством, он все же представляет совсем другой вид компьютерных атак. Кибертерроризм планируется с иными целями, такими как нанесение крупного ущерба жизненно важным объектам инфраструктуры посредством использования информационных технологий.

Для нашей страны в настоящее время актуальны все три упомянутых вида деятельности. Но самым распространенным из них является простая активность террористов в Интернете. Специализированное подразделение Министерства внутренних дел Российской Федерации, согласно законодательству, постоянно закрывает сайты с негативным контентом, который противоречит российскому законодательству. Однако впоследствии как минимум 15 % из них вновь появляются под другими именами[1].

Тем не менее в действующих российских правовых актах отсутствует определение кибертерроризма и способов его совершения. Это обстоятельство признается современными учеными в качестве одного из главных проблемных факторов выявления и противодействия кибератакам.

Изучив материал по данной теме в учебной литературе, научных статьях, а также в законодательстве можно попытаться сделать определение понятия «кибертерроризм». Таким образом, кибертерроризм – это умышленное преступное посягательство на информационный ресурс либо использование этого ресурса с целью устрашения населения, создания опасной обстановки, влекущей гибель людей, причинение значительного имущественного ущерба, либо наступления иных тяжких последствий путем воздействия на принятие решения органами государственной власти.

Список литературы

1. Веленгурин В. И. Внимание! Кибертерроризм // Вестник МЧС. 2016. № 2 (92). С. 6–19.
2. Капитонова Е. А. Особенности кибертерроризма как новой разновидности террористического акта // Известия высших учебных заведений. Поволжский регион. № 2 (34). С. 29–41.
3. Карамова Э. И. К вопросу о кибертерроризме в глобализирующемся мире // Социально-политические науки. № 3. С. 144–155.

[1] См.: Веленгурин В. И. Внимание! Кибертерроризм // Вестник МЧС. 2016. № 2 (92). С. 8.

М. Р. Булавина

К ВОПРОСУ О НЕКОТОРЫХ НЕДОСТАТКАХ ЗАКОНОДАТЕЛЬСТВА ОБ ОТВЕТСТВЕННОСТИ ЗА СОВЕРШЕНИЕ ПРЕСТУПЛЕНИЙ ЭКСТРЕМИСТСКОЙ НАПРАВЛЕННОСТИ С ИСПОЛЬЗОВАНИЕМ СРЕДСТВ МАССОВОЙ ИНФОРМАЦИИ И ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ, ВКЛЮЧАЯ СЕТЬ ИНТЕРНЕТ

Аннотация: В данной статье рассмотрены отдельные недостатки действующего уголовного законодательства об ответственности за определенные виды преступлений экстремистской направленности.

Ключевые слова: преступления экстремистской направленности, уголовный закон, уголовная ответственность, информационно-телекоммуникационные сети, сеть Интернет.

TO THE QUESTION OF SOME DEFICIENCIES IN LEGISLATION ON LIABILITY FOR EXTREMIST CRIMES USING MASS MEDIA AND INFORMATION AND TELECOMMUNICATION NETWORKS, INCLUDING THE INTERNET

Abstract: This article considers certain shortcomings of the current criminal legislation on liability for certain types of extremist crimes.

Keywords: extremist crimes, criminal law, criminal liability, information and telecommunication networks, Internet.

Информационные технологии проникают в нашу жизнь с каждым годом все больше и больше. В соответствии с Указом Президента РФ приоритетным направлением внутренней и внешней политики является «создание условий для формирования в Российской Федерации общества знаний»[1]. Формированию последнего будет способствовать усовершенствование информационно-коммуникационных технологий, а также формирования необходимой инфраструктуры[2].

[1] Указ Президента РФ от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» // СПС «Консультант Плюс», 2021.

[2] См.: Деятельность органов внутренних дел по борьбе с преступлениями, совершенными с использованием информационных, коммуникационных и высоких технологий: учебное пособие: в 2 ч. / [А. В. Аносов и др.]. М.: Академия управления МВД России, 2019. С. 5.

Но в то же время информационные технологии используются не только в благих целях. В настоящий момент все больше преступлений совершается с применением сети Интернет, в том числе преступлений экстремистской направленности[1].

При этом практика показывает, что нормы права часто требуют обновления и систематизации, так как законодатель не всегда успевает реагировать на возникающие в общественных отношениях изменения, при этом в результате анализа деятельности органов внутренних дел было выявлено, что меры, принимаемые уполномоченными органами, являются недостаточными[2]. Таким образом, актуальность изучения и анализа положений законодательства об ответственности за совершение преступлений экстремистской направленности с использованием информационно-телекоммуникационной сети Интернет очевидна[3].

Необходимо отметить, что преступления, совершаемые с использованием информационно-коммуникационных технологий, в том числе сети Интернет, имеют специфические особенности. Действия, совершаемые преступниками с использованием современных технологий, трудно обнаружить, в связи с тем, что интернет-пространство выходит за пределы конкретного государства, предоставляя возможность беспрепятственно посягать на права и интересы личности, безопасность общества и государства, что во много раз увеличивает степень опасности преступлений, совершаемых с применением информационных технологий.

Одними из наиболее опасных преступлений, посягающих на безопасность общества и государства, являются преступления экстремистской направленности, которые совершаются по мотивам расовой, религиозной, национальной, политической либо идеологической ненависти или вражды, также ненависти или вражды по отношению к определенной социальной группе.

---

[1] См.: Кобец П. Н., Краснова К. А. О современных информационных технологиях, используемых экстремистскими и террористическими организованными группами, и необходимости противодействия киберпреступности // Вестник Дальневосточного юридического института МВД России. 2018. № 2 (43). С. 75–79.

[2] План реализации решений Координационного совещания руководителей правоохранительных органов Российской Федерации от 23 сентября 2016 года «Об эффективности работы по выявлению, пресечению, расследованию и предупреждению преступлений, совершаемых с использованием современных информационно-телекоммуникационных технологий», утв. распоряжением МВД России от 12 декабря 2016 г. № 1/13128. URL: https://internet.garant.ru/#/document/77453391/paragraph/42/doclist/5091/showentries/ false/highlight/ (дата обращения: 19.01.2021).

[3] См.: Решняк М. Г. Современные проблемы действия уголовного законодательства России и отдельных зарубежных стран, связанные с цифровизацией преступной деятельности // Безопасность бизнеса. 2020. № 6. С. 54–61.

В настоящий момент преступления данной категории почти всегда совершаются с использованием современных информационно-телекоммуникационных технологий, в результате чего законодатель определил применение информационно-телекоммуникационных технологий как способ совершения преступлений в следующих статьях УК РФ: ч. 2 ст. 280 – осуществление призывов к экстремистской деятельности с использованием средств массовой информации или информационно-телекоммуникационных сетей; ч. 2 ст. 280.1 – публичные призывы к осуществлению действий по подрыву территориальной целостности РФ с использованием средств массовой информации или информационно-телекоммуникационных сетей; ч. 1 ст. 282 – возбуждение ненависти, вражды, а равно унижение человеческого достоинства, совершенные с использованием средств массовой информации, электронных или информационно-телекоммуникационных сетей, включая Интернет.

При этом в ст. ст. 280 и 280.1 УК РФ использование «средств массовой информации либо информационно-телекоммуникационных сетей, в том числе сети Интернет» является квалифицирующим признаком, а в ст. 282 – конститутивным признаком основного состава преступления. Исходя из этого, видно, что уровень общественной опасности сходных по проявлению действий экстремистской направленности оценивается законодателем по-разному. Подобное решение не является обоснованным и демонстрирует нарушение принципа системности права при рассмотрении вопроса, связанного с совершением экстремистских преступлений с использованием информационно-телекоммуникационных сетей (в том числе сети Интернет)[1].

Также необходимо обратить внимание на то, что в ч. 2 ст. 280.1 УК РФ говорится не только об использовании средств массовой информации, информационно-телекоммуникационных сетей (в том числе сети Интернет), но и об использовании электронных сетей, что не указано в ч. 2 ст. 280 и в ч. 1 ст. 282. Это свидетельствует о нарушении системности при рассмотрении составов преступлений данных правовых норм, не позволяя единообразно истолковать подход, который был применен законодателем.

Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»[2] закрепил

[1] Решняк М. Г. Уголовное законодательство об ответственности за преступления экстремистской направленности, совершаемые с использованием информационно- коммуникационных технологий: тенденции развития // Современное право. 2019. № 1. С. 103.

[2] Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // СЗ РФ от 31 июля 2006 года № 31 (часть I) ст. 3448.

понятие «**информационно-телекоммуникационная сеть**», что позволило использовать его в УК РФ. В то же время важно отметить, что Федеральный закон от 27.07.2006 № 149-ФЗ не раскрывает понятия «электронная сеть», но содержит в себе понятия «электронное сообщение» и «электронный документ», определяя их как «информацию, переданную» (электронный документ) или переданную и полученную (электронное сообщение) при помощи информационно-телекоммуникационных сетей. Некоторые авторы приходят к выводу, что «электронная сеть» и «информационно-телекоммуникационная сеть» – тождественные понятия[1], поэтому использование понятия «электронная сеть» в данной правовой норме является тавтологичным.

Рассмотрев нормы, в которых отдельным признаком состава преступления экстремистской направленности является использование лицом, совершавшим посягательство на общественную и государственную безопасность, средств массовой информации, информационно-телекоммуникационных сетей, включая сеть Интернет, можно сделать вывод, что законодательная база в целом отражает изменения, происходящие в общественных отношениях, но в то же время некоторые нормы нуждаются в корректировке и приведении к системности и последовательности.

Список литературы

1. Деятельность органов внутренних дел по борьбе с преступлениями, совершенными с использованием информационных, коммуникационных и высоких технологий: учебное пособие: в 2 ч. / [А. В. Аносов и др.]. М.: Академия управления МВД России, 2019. Ч. 1. 208 с.
2. Кобец П. Н., Краснова К. А. О современных информационных технологиях, используемых экстремистскими и террористическими организованными группами, и необходимости противодействия киберпреступности // Вестник Дальневосточного юридического института МВД России. 2018. № 2 (43). С. 75–79.
3. Ковлагина Д. А. Понятие «электронные сети» в контексте некоторых составов преступлений, предусмотренных Уголовным Кодексом РФ // Молодой ученый. 2016. № 16 (120). С. 249–251.
4. Решняк М. Г. Уголовное законодательство об ответственности за преступления экстремистской направленности, совершаемые с использованием информационно-коммуникационных технологий: тенденции развития // Современное право. 2019. № 1. С. 102–105.
5. Решняк М. Г. Современные проблемы действия уголовного законодательства России и отдельных зарубежных стран, связанные с цифровизацией преступной деятельности // Безопасность бизнеса. 2020. № 6. С. 54–61.

[1] См.: Ковлагина Д. А. Понятие «электронные сети» в контексте некоторых составов преступлений, предусмотренных Уголовным Кодексом РФ // Молодой ученый. 2016. № 16 (120). С. 250.

В. С. Кекко

ПРОБЛЕМНЫЕ ВОПРОСЫ ПРАВОВОЙ РЕГЛАМЕНТАЦИИ СПОСОБОВ ДОВЕДЕНИЯ ДО САМОУБИЙСТВА ПОСРЕДСТВОМ ИСПОЛЬЗОВАНИЯ СОЦИАЛЬНЫХ СЕТЕЙ

Аннотация: В статье анализируются существующие в юридической литературе точки зрения о причинах, условиях и способах доведения человека до совершения самоубийства посредством социальных сетей, раскрываются виды, формы проявлений унижений, угроз и оскорблений в сети Интернет. Раскрываются особенности норм Уголовного кодекса Российской Федерации в части ответственности при доведении до самоубийства, исследуются проблемные вопросы законодательного регламентирования современных способов доведения до самоубийства посредством социальных сетей.

Ключевые слова: самоубийства, социальные сети, уголовное право, киберпреступность.

PROBLEMATIC ISSUES OF LEGAL REGULATION OF METHODS OF COMMUNICATION TO SUICIDE THROUGH THE USE OF SOCIAL MEDIA

Abstract: The article analyzes the existing legal literature points of view on the causes, conditions and methods of bringing a person to commit suicide through social networks, reveals the types and forms of manifestations of humiliation, threats and insults on the Internet. The article reveals the features of the norms of the Criminal Code of the Russian Federation in terms of responsibility for bringing to suicide, examines the problematic issues of legislative regulation of modern methods of bringing to suicide through social networks.

Keywords: suicide, social media, criminal law, cybercrime.

Согласно п. 1, ст. 20 Конституции Российской Федерации каждый имеет право на жизнь[1]. В отечественной и мировой литературе есть достаточное количество исследований на эту тему, а в исторической ретроспективе можно увидеть эволюцию права человека на жизнь – от этапа «человек есть раб», когда его жизнь – собственность другого, до современной оценки жизни как основополагающей ценности общества и гражданина. На признании этого постулата строится вся система прав, свобод и ценностей человечества. В этой связи важной задачей является

[1] Конституция Российской Федерации. Принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) // СПС «Консультант плюс», 2021.

уменьшение рисков преждевременного ухода из жизни, в том числе по причинам криминогенного характера: убийств, суицидов и др. Для решения указанной задачи государство в лице соответствующих органов предпринимает серьезные профилактические меры. При этом одной из наиболее актуальных и одновременно сложных задач выступает противодействие доведению до самоубийства, прежде всего, посредством использования социальных сетей.

В 2020 году в России произошло 23 тысячи самоубийств, а вместе с попытками их совершения цифра достигает 45 тысяч и составляет 31 самоубийство на 100 тысяч населения, что ставит нашу страну на 2-е место по количеству суицидов в мире[1]. Из анализа данных о лицах, совершивших суицид, видно, что отсутствует четкая характеристика социального портрета самоубийцы. Любые возраст, профессия, семейное положение, уровень достатка присущи этой жизненной трагедии. При этом важным при проведении доследственных проверок и расследований по фактам самоубийств является изучение причин и условий, которые толкнули человека на поступок, в результате которого он покончил жизнь самоубийством. Немаловажным в этой связи является исследование фактов, а также способов доведения до самоубийства, ведь принять решения прекратить жить без внешнего давления (за исключением сложных психических отклонений) человек вряд ли мог. Вместе с тем мы видим, что в современных условиях жизни человека, где виртуальное пространство уверенно замещает реальное, случаи доведения до самоубийства посредством социальных сетей неуклонно увеличиваются. Опросы показали, что в 2020 году в среднем пользователь проводил в социальных сетях от трех до пяти часов в день[2]. При этом именно прошлый год, связанный со сложной эпидемиологической обстановкой и принятием мер ограничительного характера, увеличил этот показатель в разы. Все это заставляет обратить самое пристальное внимание на изучение способов доведения до самоубийства посредством социальных сетей.

Логичной выглядит аксиома, что последствия любого рода унижений являются фатальными для личности и ее самооценки. Сложнее,

[1] В 2020 году Россия занимает 2-е место по количеству самоубийств в мире, уступая Литве. URL: https://zen.yandex.ru/media/myprotest/v-2020-godu-rossiia-zanimaet-2-mesto-po-kolichestvu-samoubiistv-v-mire-ustupaia-litve-5f85a19401c3532acc2cebf2 (дата обращения: 04.01.2021).

[2] Сколько человек проводит время в Интернете? // BigLions. URL: https://service-seo.com/skolko-chelovek-provodit-vremya-v-internete/ (дата обращения: 04.01.2021).

с точки зрения правовой оценки, обстоят дела с унижениями чести и достоинства личности на просторах Интернета. Анализируя эту ситуацию, Н. Подольски приходит к выводу, что «… в большинстве стран наблюдается законодательный вакуум в этой сфере, что приводит к безнаказанности данного рода преступлений. Лишь некоторые авторы проводят исследования в разных странах по исследуемой проблеме, но и они не имеют практического применения в правовом поле, так как сложно очертить рамки и грани преступления в сфере унижения в виртуальном публичном месте»[1].

Вместе с тем в России уже в 2017 году были внесены изменения в нормы Уголовного кодекса, касающиеся привлечения виновных лиц к ответственности за доведение до самоубийства. 7 июня 2017 года Федеральным законом № 120-ФЗ установлены дополнительные механизмы противодействия деятельности, направленной на побуждение людей к суицидальному поведению[2]. Данным Федеральным законом ст. 110 УК РФ («доведение до самоубийства») дополнена ч. 2, куда включен отягчающий квалифицирующий признак доведения до самоубийства в публичном выступлении, публично демонстрирующемся произведении, средствах массовой информации или информационно-телекоммуникационных сетях (включая сеть Интернет).

Рассматриваемые изменения в УК РФ отражают понимание общественной опасности от неконтролируемой информатизации населения, ее криминогенное влияние на индивидуальное и коллективное сознание, выражающееся в нарушении норм права, морали и этики в социальных сетях. По нашему мнению, государство в этом вопросе еще не реализовало свои полномочия в полной мере. Для обоснования заявленной позиции, основываясь на изученной правоприменительной практике, попытаемся раскрыть существующие способы доведения до самоубийства в социальных сетях.

В рамках настоящего исследования актуальным является рассмотрение такого понятия, как «киберунижение», целью которого является

[1] См.: Подольски Н. Социальные истоки унижения в интернет-пространстве // Социальная реальность виртуального пространства. Материалы I Международной научно-практической конференции / Под общ. ред. О. А. Полюшкевич, Г. В. Дружинина. Иркутск, 2019. С. 375.

[2] Федеральный закон от 07.06.2017 № 120-ФЗ«О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации в части установления дополнительных механизмов противодействия деятельности, направленной на побуждение детей к суицидальному поведению» // СПС «Консультант Плюс», 2021.

уничтожение личности человека в Сети посредством критических высказываний, оскорблений, унижений, угроз и шантажа. Все это приводит к тому, что человек, в отношении которого применяется такое «нападение», перестает пользоваться авторитетом и уважением[1]. В качестве примера можно привести создание от имени пользователя-жертвы аккаунта, который содержит отличительную от реальных данных информацию, отталкивающую других пользователей; удаление аккаунта пользователя или его группы, что воспринимается потерпевшим как попытка виртуального «убийства»; необоснованная критика жертвы с использованием нецензурных фраз (может происходить отдельным пользователем или группой пользователей); выгрузка в социальные сети реальных или смонтированных фото, видеоматериалов, которые входят в личную, интимную или служебную зону пользователя.

Все это направлено на необоснованное унижение чести и достоинства человека в Сети посредством представления вымышленной и несоответствующей действительности информации в качестве реальной, что в своем итоге приводит к разрушению психологической основы личности большинства интернет-пользователей. При этом выставленная в Сеть информация не соответствует действительной, под сомнение ставится репутация человека. Особенно актуален этот вопрос по отношению к несовершеннолетним, для которых Интернет заменяет зачастую реальную жизнь. В конечном итоге интернет-унижения приводят к депрессивному состоянию, отсутствию радости и перспектив жизни и, как следствие, ощущению покинутости, что в свою очередь приводит к признакам суицидального поведения.

Развивая тему киберунижения, необходимо отметить, что похожим по способу доведения до суицида в интернет-пространстве являются: киберпреследование, киберзапугивание, психологическое насилие и bashing.

Киберпреследование – это использование ресурсов социальных сетей для домогательства в отношении конкретного человека или группы людей по социальным, национальным, расовым и другим признакам[2]. При таком преследовании используется распространение ложных слухов о человеке, сплетен, а также клеветы.

К киберпреследованию также относится информационное похищение личности (аккаунта пользователя), интернет-вандализм, иные проявления домогательств в социальных сетях.

---

[1] См.: Подольски Н. Указ. соч. С. 375.

[2] См.: Рерке В. И., Портная Я. А. Психологические особенности троллеров социальных сетей // Казанский педагогический журнал. 2019. № 4. С. 155.

Под киберзапугиванием понимается использование технологий интернет-пространства с целью угроз и шантажа потерпевшего. При киберзапугивании могут использоваться агрессивные тексты, твитты или сообщения[1]. Психологическое насилие – это выгрузка в социальные сети фото, видеофайлов, на которых зафиксировано избиение или приставание к человеку. Суть понятия bashing заключается в систематической публичной необоснованной критике человека в социальных сетях. При этом используются ненормативная лексика, непристойные фото и видеоизображения[2].

Возможность причинения личностного ущерба посредством унижений в социальных сетях возникает в случае подмены образа человека в реальной жизни с его образом в виртуальном пространстве. Пользователь начинает существовать больше в социальной сети, чем в обычных условиях, меняются его приоритеты и ценностные ориентиры. По мнению Ж. Бодрийяра, «образ начинает заражать реальность и моделировать ее»[3]. Особенностью интернет-пространства является слабая идентификация его пользователей, когда указываются вымышленные персональные данные, не загружаются реальные фото человека. Все это приводит к чувству безнаказанности и возможности проявлять самые низменные качества. Еще одной особенностью киберунижения является возможность коллективного «изобличения» жертвы, когда один пользователь выставляет ложную информацию о человеке, а остальные поддерживают его посредством комментариев, в том числе с развитием темы обсуждения.

Из вышесказанного следует, что главным местом, где происходит кибербуллинг, являются социальные сети, в которых уровень интернет-взаимодействия высок, существует большое количество групп, которые пользователь может выбрать себе в зависимости от интересов. При этом опасность киберзапугивания относительно издевательств в реальной жизни намного выше, в связи с более широким кругом возможных жертв через социальные сети, мессенджеры и уязвимости потерпевших. Все это увеличивает количество противоправных действий в Интернете, размывая чувство ответственности и легкость достижения целей, связанных с человеческим унижением.

---

[1] См.: Рерке В. И., Маякова О. С. К вопросу развития социальной активности подростков как условия их психологической безопасности // Baikal Research Journal. 2019. Т. 10. № 2. С. 110.

[2] См.: Рерке В. И., Портная Я. А. Указ. соч. С. 156.

[3] См.: Дьяков А. В. Жан Бодрийяр: стратегии «радикального мышления» / Под ред. А. С. Колесникова. СПб.: Изд-во С.-Петерб. ун-та, 2008. С. 312.

Сложившаяся в настоящее время ситуация, связанная с преступлениями такого рода, свидетельствует о том, что именно способы доведения до самоубийства в социальных сетях являются превалирующими среди всех способов совершения данного преступления в целом. Это связано с современной спецификацией образа жизни и коммуникативных связей между людьми. В свою очередь это приводит к существенной проблеме, связанной с киберунижениями во всех его видах. Причиной этого служит отсутствие рычагов влияния на пользователей в части идентификации их реальных данных, контроля и цензуры их поведения в Сети, а также критических высказываний, мониторинга и оперативного блокирования информации, вредящей репутацию и имиджа человека. Важным направлением предупреждения данной категории преступлений является виктимологическая сторона, связанная с поведением потерпевшего, нахождением в виртуальном пространстве все свободное время, а также замкнутостью при появлении проблем с другими пользователями социальных сетей. Это в первую очередь присуще несовершеннолетним жертвам. В этой связи важна роль родителей и органов профилактики нарушений среди несовершеннолетних, которые обязаны принимать непосредственное участие как в реальной, так и виртуальной жизни подростка.

В связи с быстрым развитием интернет-пространства, постоянным изменением способов доведения до самоубийства, вероятностью появления новых их видов, связанных с развитием интернет-технологий, требуется законодательная регламентация подобного рода противоправных деяний, в первую очередь в части, касающейся более детального раскрытия и закрепления в уголовном законе способов доведения до самоубийства посредством социальных сетей.

Из диспозиции ст. 110 УК РФ мы видим, что доведение лица до самоубийства или до покушения на самоубийство может происходить в публичном выступлении, публично демонстрирующемся произведении, средствах массовой информации или информационно-телекоммуникационных сетях (включая сеть Интернет) путем угроз, жестокого обращения или систематического унижения человеческого достоинства потерпевшего. При этом законодателем не раскрываются иные способы совершения подобного рода преступлений, таких как, например, киберунижений, возникающих в повседневной практике, и о которых велась речь выше. Такая же тенденция присуща правоприменительной и судебной практике по указанной категории уголовных дел, что также усложняет работу по доказыванию вины лиц, причастных к доведению

до самоубийства. Все это способствует уходу от ответственности киберпреступников.

Важной стороной предупреждения указанной категории преступлений является разработка действенного механизма контроля и мониторинга социальных сетей на предмет выявления унижений. В данных обстоятельствах необходимым является применение санкций в отношении ответственных за организацию конкретных социальных сетей («Вконтакте», «Одноклассники», «Инстаграм», «ТикТок» и др.). Нужна регламентация процесса наложения ограничений работы интернет-ресурсов в связи с наличием не удаленной определенное время информации, содержащей факты унижений, угроз, оскорблений в отношении того или иного лица. Важно также ввести обязанность для администраторов социальных сетей направлять сведения о потенциальных интернет-преступниках. Информация о таких гражданах и их противоправной деятельности в социальных сетях должна передаваться в правоохранительные органы для проведения проверки в соответствии со ст. 144–145 УПК РФ, а их аккаунты блокироваться.

Таким образом, на наш взгляд, для решения проблемы противодействия способам доведения до самоубийства посредством социальных сетей необходим комплексный подход, подразумевающий применение мер уголовного, криминогенного, информационно-технологического и педагогического характера.

Список литературы

1. Дьяков А. В. Жан Бодрийяр: стратегии «радикального мышления» / Под ред. А. С. Колесникова. СПб.: Изд-во С.-Петерб. ун-та, 2008. 389 с.
2. Ережипалиев Д. И., Краснова К. А. Противодействие кибербуллициду как средство предупреждения суицидов несовершеннолетних // Юристъ-Правоведъ. 2017. № 3 (82). С. 78–84.
3. Подольски Н. Социальные истоки унижения в интернет-пространстве // Социальная реальность виртуального пространства. Материалы I Международной научно-практической конференции / Под общ. ред. О. А. Полюшкевич, Г. В. Дружинина. Иркутск, 2019. С. 374–378.
4. Рерке В. И., Маякова О. С. К вопросу развития социальной активности подростков как условия их психологической безопасности // Baikal Research Journal. 2019. Т. 10. № 2. DOI: 10.17150/2411- 6262.2019.10(2).7 11.
5. Рерке В. И., Портная Я. А. Психологические особенности троллеров социальных сетей // Казанский педагогический журнал. 2019. № 4. С. 155–160.

Раздел II

СЕКЦИЯ «ПРОБЛЕМЫ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПНОСТИ»

В. А. Аксенов

ПРОФИЛАКТИКА МОШЕННИЧЕСТВА, СОВЕРШЕННОГО С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ НА ТЕРРИТОРИИ ИСПРАВИТЕЛЬНОГО УЧРЕЖДЕНИЯ

Аннотация: Целью данного исследования является рассмотрение проблемы совершения мошеннических действий с использованием информационно-коммуникационных технологий с территории исправительных учреждений системы ФСИН России. Изучены меры, применяемые ФСИН России совместно с операторами сотовой связи в целях профилактики осуществления звонков с территории исправительных учреждений.

Ключевые слова: информационно-коммуникационные технологии, исправительное учреждение, мошенничество, профилактика.

PREVENTION OF FRAUD COMMITTED USING INFORMATION AND COMMUNICATION TECHNOLOGIES ON THE TERRITORY OF THE CORRECTIONAL INSTITUTION

Abstract: The purpose of this study is to consider the problem of committing fraud using information and communication technologies from the territory of correctional institutions of the Federal Penitentiary Service of Russia. The measures used by the Federal Penitentiary Service of Russia in conjunction with mobile operators to prevent calls from the territory of correctional institutions were studied.

Keywords: information and communication technology, correctional facility, fraud, prevention.

В условиях развития пенитенциарной системы РФ важную роль занимают положения выполнения в исправительных учреждениях системы ФСИН России социально-воспитательных и психологических функций, а также исправления и предупреждения совершения новых преступлений осужденными лицами. Следствием увеличения общего количества мошенничеств, совершенных с использованием информационно-коммуникационных

технологий, явилось пополнение пенитенциарных учреждений преступниками, осужденными за совершение преступлений данной категории. Во многих случаях интернет-мошенники, содержащиеся в пенитенциарных учреждениях, становятся «учителями» для своих сокамерников, разъясняя схемы и методики совершения мошенничеств, как правило, с использованием средств сотовой и иной связи.

Основные признаки преступлений данной категории:

1. Преступник в момент совершения преступления уже отбывает наказание за совершение иного преступного деяния. Злоумышленник содержится на территории исправительного учреждения системы ФСИН России под контролем и охраной со стороны сотрудников пенитенциарной системы.
2. Объект преступного посягательства располагается за пределами исправительного учреждения. То есть преступление, как правило, латентно для сотрудников пенитенциарной системы и не затрагивает интересы самого исправительного учреждения.
3. Между злоумышленником и жертвой преступления имеется территориальная дистанция[1].

В текущем году в средствах массовой информации РФ стали появляться публикации о расположении в исправительных учреждениях системы ФСИН России колл-центров, в которых лица, отбывающие наказания в виде лишения свободы или содержащиеся под стражей на период проведения следственных действий, совершают мошеннические действия от имени сотрудников банков под предлогом приостановления подозрительных операций. 29 сентября 2020 года заместитель председателя правления ПАО «Сбербанк» С. К. Кузнецов сообщил, что 40–50 % преступных колл-центров находится в исправительных учреждениях системы ФСИН России, а их доходы составляют более 75 млн рублей в месяц[2].

Основными профилактическими мерами, принимаемыми Центральным Банком России для уменьшения количества проведения финансовых операций без согласия клиента, являются:

- совершенствование законодательства РФ в сфере обеспечения информационной безопасности финансово-кредитных учреждений;

[1] См.: Литвинов Н. Д., Федоров А. Н. Особенности, причины и тенденции развития дистанционного мошенничества лицами, отбывающими наказание в местах лишения свободы // Научно-исследовательские публикации. 2015. № 12 (32). С. 65.

[2] См.: Полтавская Е. Доход мошенников – более 75 млн рублей в месяц. URL: https://iz.ru/1066654/elena-poltavskaia/dokhod-moshennikov-bolee-75-mln-rublei-v-mesiatc (дата обращения: 19.01.2021).

- совершенствование нормативных актов Центробанка РФ в сфере информационной безопасности финансово-кредитных учреждений;
- повышение финансовой грамотности населения РФ в сфере безопасности используемых информационных и платежных технологий;
- организация информационного обмена на базе подразделения Центрального банка России – ФинЦЕРТа в целях обеспечения быстрого и постоянного уведомления об угрозах нарушения информационной безопасности, а также о проведении финансовых операций без согласия клиентов1.

09 сентября 2020 года депутатами Государственной думы РФ А. Е. Хинштейном, В. И. Пискаревым, П. В. Крашенинниковым и А. А. Гетта на обсуждение представлен законопроект «О внесении изменений в отдельные законодательные акты Российской Федерации в части прекращения оказания услуг связи на территории учреждений, исполняющих уголовные наказания в виде лишения свободы, и мест содержания под стражей», который в настоящее время одобрен в первом чтении[2].

Для понимания того, как осуществляется блокирование вызовов абонентов, находящихся на территории исправительных учреждений системы ФСИН России, рассмотрим актуальные разработки оборудования и программного обеспечения в данном направлении. В целях пресечения деятельности преступных колл-центров, расположенных на территории исправительных учреждений, операторами сотовой связи разработан комплекс специального оборудования, запрещающего осуществление звонков, в состав которого входят следующие элементы:

1. «ПАК ИП – БЛК», представляющий собой многоканальный блок буферных базовых станций GSM (глобальная система мобильной связи), работающих на сетевых кодах MNC операторов сотовой связи, имеющих покрытие на защищаемой территории (в нашем случае территории исправительных учреждений).

[1] Обзор операций, совершенных без согласия клиентов финансовых организаций за 2019 год. URL: https://www.cbr.ru/Content/Document/File/103609/Review_of_transactions_2019.pdf (дата обращения: 19.01.2021).

[2] Система обеспечения законодательной деятельности государственной автоматизированной системы «Законотворчество». Законопроект № 876381-7 «О внесении изменений в отдельные законодательные акты Российской Федерации в части прекращения оказания услуг связи на территории учреждений, исполняющих уголовные наказания в виде лишения свободы, и мест содержания под стражей». URL: https://sozd.duma.gov.ru/bill/876381-7 (дата обращения: 19.01.2021).

2. Универсальный постановщик целевых цифровых помех под названием «Контур-Ф». Основными целями работы данного оборудования являются: подавление сигналов LTE (стандарт беспроводной высокоскоростной передачи данных для мобильных телефонов и других терминалов) для принуждения мобильных телефонов, находящихся на территории исправительных учреждений, переключения на систему «ПАК ИП – БЛК» (режим селективной скрытной буферизации нелегальной сотовой связи); подавление других каналов работы запрещенных на территории исправительного учреждения мобильных телефонов (Wi-Fi и DEC); подавление сигналов GSM (режим полного запрета сотовой связи); отсутствие помех радиосвязи (типа Tetra) на территории исправительного учреждения.
3. Сенсор мониторинга радиоэлектронной обстановки «Контур-М», который позволяет в режиме реального времени осуществлять мониторинг радиоэлектронной обстановки на объекте, выявлять сигналы новых каналов утечки, возникших после развертывания системы, после чего происходит их пеленгация и передача в систему «Контур-Ф».
4. Терминал управления данной системой.

Схема работы систем «ПАК ИП – БЛК» и «Контур», препятствующих осуществлению звонков с мобильных устройств, находящихся на территории исправительных учреждений, выглядит следующим образом:

- на автоматизированном рабочем месте вводится или активируется заранее введенный «белый» список доверенных абонентов;
- все остальные абоненты, расположенные в зоне действия оборудования – исправительного учреждения, являются недостоверными;
- после включения оборудования мобильные телефоны абонентов с включенным режимом LTE теряют связь со своими базовыми станциями;
- мобильные телефоны переключаются на систему «ПАК ИП – БЛК» как новую базовую станцию сети;
- далее мобильные телефоны автоматически посылают запрос на регистрацию в систему «ПАК ИП – БЛК»;
- мобильным телефонам, внесенным в список доверенных абонентов, указанная система отказывает в регистрации, и они автоматически перестраиваются на GSM – базовые станции

собственных сетей, оставаясь при этом на связи. При этом мобильным устройствам, не внесенным в список доверенных абонентов, автоматическая регистрация в системе разрешается;

- далее абонент попадает в буферную базовую станцию системы «ПАК ИП – БЛК» без возможности ручного выбора GSM базовых станций собственных сетей и становится недоступным для входящих звонков;
- при попытке осуществить звонок с мобильного телефона, находящегося на территории исправительного учреждения, абонент получит сообщение от автоответчика (пример: «Данный вид связи недоступен для абонента»). Все попытки осуществления исходящих звонков от недостоверных абонентов регистрируются на автоматизированном рабочем месте;
- попытки абонентов искать публичные каналы Wi-Fi или Wimax-соединений пресекаются системой «Контур-Ф».

Таким образом, внесение изменений в законодательство РФ в части прекращения оказания услуг связи на территории учреждений, исполняющих уголовные наказания в виде лишения свободы, и мест содержания под стражей является действенной мерой профилактики мошенничеств, совершенных с использованием информационно-коммуникационных технологий.

Список литературы

1. Литвинов Н. Д., Федоров А. Н. Особенности, причины и тенденции развития дистанционного мошенничества лицами, отбывающими наказание в местах лишения свободы // Научно-исследовательские публикации. 2015. № 12 (32). С. 63–72.
2. Полтавская Е. Доход мошенников – более 75 млн рублей в месяц. URL: https://iz.ru/1066654/elena-poltavskaia/dokhod-moshennikov-bolee-75-mln-rublei-v-mesiatc (дата обращения: 19.01.2021).
3. Обзор операций, совершенных без согласия клиентов финансовых организаций за 2019 год. URL: https://www.cbr.ru/Content/Document/File/103609/Review_of_transactions_2019.pdf (дата обращения: 19.01.2021).
4. Система обеспечения законодательной деятельности государственной автоматизированной системы «Законотворчество». Законопроект № 876381-7 «О внесении изменений в отдельные законодательные акты Российской Федерации в части прекращения оказания услуг связи на территории учреждений, исполняющих уголовные наказания в виде лишения свободы, и мест содержания под стражей». URL: https://sozd.duma.gov.ru/bill/876381-7 (дата обращения: 19.01.2021).

С. Р. Бендас

КИБЕРПРЕСТУПНОСТЬ И КОРОНАВИРУСНАЯ ИНФЕКЦИЯ COVID-19: РИСКИ И ОТВЕТНЫЕ МЕРЫ

Аннотация: В данной статье рассматривается актуальная проблема влияния новой коронавирусной инфекции COVID-19 на состояние преступлений в сфере информационной безопасности, приведена краткая статистика киберпреступлений за 2020 год, указаны причины снижения активности правоохранительных органов, направленной на расследование киберпреступлений, а также перечислены новейшие виды преступлений и способы противодействия им со стороны государства.

Ключевые слова: киберпреступность, информационная безопасность, онлайн-мошенничество, инфодемия.

CYBERCRIME AND COVID-19: RISKS AND RESPONSES

*Abstract***:** This article discusses the current problem of the impact of the new coronavirus infection COVID-19 on the state of crimes in the field of information security, provides brief statistics of cybercrimes for 2020, indicates the reasons for the decrease in the activity of law enforcement agencies aimed at investigating cybercrimes, and also lists the latest types of crimes and methods of counteraction. them from the state.

Keywords: cybercrime, information security, online fraud; infodemia.

На сегодняшний день в большинстве стран мира применены комплексные меры социального дистанцирования. Данные меры привели к заметному возрастанию числа использования средств онлайн-коммуникаций правительственными учреждениями, крупными корпорациями и мелкими предприятиями, отдельными лицами. Для некоторых из них работа в онлайн-сервисах в таком крупном масштабе осуществляется впервые. Именно эта группа является самым привлекательным и уязвимым контингентом для киберпреступников и хакеров. По причине нахождения на удаленной работе и дистанционном обучении, в Интернете растет число пользователей, которые недостаточно проинформированы об угрозах и в большей мере подвергают себя опасности, находясь в домашних условиях, чем на работе или в учебном заведении.

В России за три месяца 2020 года число преступлений с использованием IT-технологий выросло почти на 84 % по сравнению с аналогичным периодом прошлого года[1].

Все чаще на просторах Интернета появляются рекламные объявления о поддельных лекарственных препаратах, дезинфицирующих

[1] См.: Сборник Генеральной прокуратуры о состоянии преступности в стране. URL: http://crimestat.ru/analytics (дата обращения: 15.01.2021).

средствах, средствах индивидуальной защиты, гигиены (негодного качества). Нередко встречаются предложения приобрести поддельные тесты или результаты теста на коронавирус.

К другим видам онлайн-мошенничества относят консультации по «выгодным» инвестициям, а также мнимые медицинские консультации и бесплатные диагностики. Некоторые преступники выдают себя за должностных лиц, представляясь, к примеру, сотрудниками банка, после чего доверчивые граждане предоставляют им данные своей банковской карты[1].

Осуществляется сбор средств «благотворительными организациями», не являющимися таковыми. Киберпреступники представляются сотрудниками благотворительных организаций и осуществляют рассылку электронных писем с просьбой помочь и перевести средства на помощь компаниям по борьбе с коронавирусом (по их словам, для проведения исследований, помощи больным, закупки медикаментов). Адресатов данных писем просят ввести данные банковской карты или провести платеж на кошелек злоумышленника.

Киберпреступники зачастую направляют свою деятельность на школьников, используя груминг[2] и сексуальный шантаж[3] в отношении детей.

Пожилые граждане, которые также слабо проинформированы об угрозах в Сети, становятся жертвами киберпреступников, которые используют их для загрузки и рассылки вирусных ссылок через электронные спам-сообщения об инфекции COVID-19.

На различных форумах «даркнета» активизировалась продажа компромата, в том числе и на госслужащих и знаменитостей. Это произошло по причине роста фишинговых атак, в результате чего к злоумышленникам в руки попадали логины и пароли пользователей, перешедших по ссылке или открывших вирусное вложение. В результате в руках киберпреступников оказывались данные, применяемые ими для шантажа их жертв.

Также там можно найти различные советы по обучению, как и на чем получать прибыль во время пандемии коронавирусной

[1] Риски отмывания денег и финансирования терроризма, связанные с COVID-19, и ответные меры в области политики / ФАТФ. 2020. URL: http://www.fatf-gafi.org/publications/methodandtrends/documents/covid-19-ML-TF.html (дата обращения: 15.01.2021).

[2] Нежелательный контакт и груминг. URL: https://www.esafety.gov.au/parents/big-issues/unwanted-contac (дата обращения: 15.01.2021).

[3] Сексуальный шантаж. URL: https://www.esafety.gov.au/key-issues/image-based-abuse/take-action/deal-with-sextortion (дата обращения: 15.01.2021).

инфекции[1]. Известны факты осуществления DDos-атак на медицинские учреждения, лаборатории, разрабатывающие и тестирующие вакцины[2].

Снижение активности правоохранительных органов, направленной на расследование киберпреступлений, объясняется переключением их внимания на расследование правонарушений и преступлений, связанных с нарушением карантинных мер. Некоторые сотрудники сами оказались инфицированными, что не позволяет им выполнять свою работу, как и сотрудникам, контактировавшим с заболевшими.

Карантинные меры сильно повлияли и на судебную систему. В России 18 марта 2020 года Президиумами Верховного Суда и Совета судей было принято постановление из-за опасности распространения коронавирусной инфекции. Судам предписывалось на неопределенный срок приостановить личный прием граждан, а все процессуальные документы рекомендовали направлять в электронном виде или по почте. Постановление также ограничило доступ на судебное заседание для всех, кроме самих участников процесса[3]. Данные меры в какой-то степени замедлили процесс судопроизводства, в том числе и борьбу с киберпреступностью.

Фейковая и ничем не подтвержденная информация относительно коронавируса распространяется в основном посредством соцсетей и мессенджеров. Модерация и строгая внутренняя политика компаний не всегда справляются с данной проблемой. Всемирная организация здравоохранения уже назвала ситуацию «инфодемией» – информационной пандемией. На ее сайте на разных языках, в том числе и на русском, разоблачаются самые популярные и порой невероятные мифы о коронавирусе, что способствует снижению числа ложных представлений о данной инфекции[4].

На помощь в данном случае приходит и местное законодательство. К примеру, в России были внесены поправки в УК РФ о штрафах или ограничении свободы за распространение заведомо ложной

[1] Риски отмывания денег и финансирования терроризма, связанные с COVID-19, и ответные меры в области политики / ФАТФ. 2020. URL: http://www.fatf-gafi.org/publications/methodandtrends/documents/covid-19-ML-TF.html (дата обращения: 15.01.2021).

[2] DDoS-атаки в первом квартале 2020 года. URL: https://securelist.ru/ddos-attacks-in-q1-2020/95949/ (дата обращения: 15.01.2021).

[3] «Вынужденный карантин»: новый вызов для судебной системы. URL: https://pravo.ru/story/219624/ (дата обращения: 15.01.2021).

[4] Фейки о коронавирусе: кому выгодно их распространять? URL: https://www.dw.com/ru/фейки-о-коронавирусе-и-комувыгодно-их-распространять/a-52654552 (дата обращения: 15.01.2021).

информации об опасных для жизни и здоровья населения обстоятельствах (ст. 207.1 УК РФ). Сюда же относится и информация о коронавирусе. Параллельно добавлено и административное наказание за такого же рода фейки (ст. 13.15 КоАП РФ).

Повышение осведомленности во время всемирной пандемии является главной задачей в процессе устранения угроз и расширения возможностей предотвращения киберпреступлений, преимущественно совершаемых в отношении самых легкоуязвимых групп населения – детей и пожилых людей. Достаточно знать основные правила при использовании Интернета:

1. Не загружать файлы из непроверенных источников.
2. Не переходить по ссылкам, содержащимся в электронных письмах от неизвестных вам отправителей.
3. Не сообщать никому свои пароли и личные данные, в том числе данные банковской карты и номер телефона[1].

Список литературы

1. «Вынужденный карантин»: новый вызов для судебной системы. URL: https://pravo.ru/story/219624/ (дата обращения: 15.01.2021).
2. DDoS-атаки в первом квартале 2020 года. URL: https://securelist.ru/ddos-attacks-in-q1-2020/95949/ (дата обращения: 15.01.2021).
3. Защитим себя от киберпреступности. URL: https://samara.sledcom.ru/Zashhitim-sebya-ot-kiberprestupnosti (дата обращения: 15.01.2021).
4. Нежелательный контакт и груминг. URL: https://www.esafety.gov.au/parents/big-issues/unwanted-contact (дата обращения: 15.01.2021).
5. Сборник Генеральной прокуратуры о состоянии преступности в стране. URL: http://crimestat.ru/analytics (дата обращения: 15.01.2021).
6. Сексуальный шантаж. URL: https://www.esafety.gov.au/key-issues/image-based-abuse/take-action/deal-with-sextortion (дата обращения: 15.01.2021).
7. Риски отмывания денег и финансирования терроризма, связанные с COVID-19, и ответные меры в области политики / ФАТФ. 2020. URL: http://www.fatf-gafi.org/publications/methodandtrends/documents/covid-19-ML-TF.html (дата обращения: 15.01.2021).
8. Фейки о коронавирусе: кому выгодно их распространять? URL: https://www.dw.com/ru/фейки-о-коронавирусе-и-комувыгодно-их-распространять/a-52654552 (дата обращения: 15.01.2021).
9. Статья посвящена актуальной, но малоизученной субкультуре хакеров, становление и популяризация которой для общества виртуализации и глобализации имеет важно значение в развитии киберпреступности, пришедшей вслед за наступлением XXI века, как нового вызова мировой науке.

[1] Защитим себя от киберпреступности. URL: https://samara.sledcom.ru/Zashhitim-sebya-ot-kiberprestupnosti (дата обращения: 15.01.2021).

И. В. Боровцов

СУБКУЛЬТУРА ХАКЕРОВ: АКТУАЛЬНОЕ СОСТОЯНИЕ И НАПРАВЛЕНИЯ РАЗВИТИЯ

Аннотация: Статья посвящена актуальной, но малоизученной субкультуре хакеров, становление и популяризация которой в обществе виртуализации и глобализации играет значительную роль в развитии киберпреступности, пришедшей вслед за наступлением XXI века, как нового вызова мировой науке.

Ключевые слова: виртуализация, киберпреступность, субкультура, хакеры, хактивизм.

HACKER SUBCULTURE: CURRENT STATE AND DEVELOPMENT DIRECTIONS

Abstract: The article is devoted to the current, but little-studied subculture of hackers, the formation and popularization of which in the society of virtualization and globalization plays a significant role in the development of a new challenge to world science – cybercrime that came after the onset of the XXI century.

Keywords: virtualization, cybercrime, subculture, hackers, hacktivism.

Сегодня всеобщая виртуализация социальной реальности и окончательное утверждение гиперреальности выступают наследием глобализирующего импульса второй половины XX века, развертываясь в полной мере в течение последних двадцати лет. Развитию киберпреступности было предпослано «необъяснимое сочетание фантазий о всемогуществе, выплескивающееся в виртуальное царство социальных медиа и Интернета»[1], из которого, благодаря технологиям децентрализованного обращения цифровых данных, в среде программистов выкристаллизовалась субкультура хакеров, изменившая взгляды на киберпреступность. Отныне она представляется не только закономерным атрибутом виртуализации, разновидностью преступности, выделяемой в связи с электронным опосредованием противозаконного поведения[2],

[1] Метамодернизм: историчность, аффект и глубина после постмодернизма / Р. ван ден Аккер: [пер. с англ. В. М. Липки; вступит. ст. А. В. Павлова]. М.: РИПОЛ классик, 2020. С. 122.

[2] За основу взято определение киберпреступления в узком смысле, выработанное в ходе Десятого Конгресса Организации Объединенных Наций по предупреждению преступности и обращению с правонарушителями (Вена, 10–17 апреля 2000 года): «любое противоправное деяние, осуществляемое посредством электронных операций, целью которого является преодоление защиты компьютерных систем и обрабатываемых ими данных». См.: Преступления, связанные с использованием

но сама во многом конструирует социальную и прежде всего политическую реальность. «В свете откровений Эдварда Сноудена наши цифровые данные стали предметом манипуляций со стороны капиталистов и пристального государственного интереса до такой степени, которую не мог бы вообразить даже параноик»[1].

Свою историю движение хакеров ведет с конца 50-х годов XX века, когда студенты и выпускники Массачусетского технологического института делали первые шаги в освоении киберпространства. В то время движение не обладало деструктивным характером, в его основе лежал ряд сходных с пацифистской повесткой субкультуры хиппи этических принципов, в числе которых как демократизм и принцип децентрализованности, направленные против некритического принятия авторитетов, так и отрицание социального неравенства и вера в возможность изменения мира к лучшему, в том числе посредством компьютерных технологий[2].

Периодизация истории субкультуры хакеров определяет ее актуальное состояние как четвертый этап развития, берущий начало на рубеже XX и XXI веков и характеризующийся институционализацией хакеров – созданием «крупных объединений, союзов, фирм, тесным образом сотрудничающих с криминальными и теневыми структурами»[3].

На четвертом этапе распространение субкультуры хакеров происходит по нескольким направлениям. Во-первых, фиксируется расширение круга лиц, имеющих доступ к технологиям, используемым хакерами: кибersталкеры, преследователи-новички, случайные интересанты, будь то уволенные работники или террористы-одиночки, – все они могут получить доступ к примитивному инструментарию хакеров, позволяющему взламывать персональные компьютеры, смартфоны и банковские счета. Возрастает охват социальных статусов, имеющих возможность приобретения необходимых технологий и обучения «ремеслу» хакера – элитарность и замкнутость, присущие ранним

компьютерной сети. Справочный документ для семинара-практикума по преступлениям, связанным с использованием компьютерной сети (A/CONF.187/10) // Десятый Конгресс Организации Объединенных Наций по предупреждению преступности и обращению с правонарушителями. Сборник документов / Сост. А. Г. Волеводз. М.: Юрлитинформ, 2001. С. 249–272.

[1] Метамодернизм… Указ. соч. С. 109.

[2] См.: Дремлюга Р. И. Субкультура хакеров и другие факторы компьютерной преступности // Криминологический журнал Байкальского государственного университета экономики и права. 2008. № 4. С. 22–26.

[3] Овчинский В. С. Криминология цифрового мира: учебник для магистратуры. М.: Норма: ИНФРА-М, 2018. С. 191.

этапам становления субкультуры, размываются и уходят в прошлое. «Это значит, что, даже находясь в тюрьме, «оснащенный» преступник может совершать безнаказанно киберпреступления»[1]. Субкультура хакеров рискует постепенно уступить место новой форме девиантности – киберпанк-субкультуре – с присущими ей специфическими ценностями, предполагающими одобрение несанкционированного и бесплатного доступа к любым компьютерным программам и их последующего пиратского тиражирования.

Во-вторых, среда «профессиональных», институционализированных хакеров окончательно приобретает черты международного бизнеса, систематически оказывающего услуги как террористическим и мафиозным организациям, так и государствам. Эта среда продолжает специализироваться и типологизироваться по разнообразным основаниям. Наиболее популярна типология, произведенная сообразно мотивам деятельности хакеров, подразделяющая их на: а) геймеров и клаберов[2]; б) спамеров; в) «белых» и г) «черных» хакеров, также именуемых кракерами, которые в свою очередь включают вандалов, шутников, экспериментаторов, взломщиков, шпионов и фишеров[3]. В зависимости от психологической характеристики девиантного самовыражения выделяются: а) пионеры – сторонники новейших технологий; б) хулиганы, компенсирующие чувство обиды; в) гедонисты, обретающие удовлетворение посредством взлома компьютерных систем; г) вандалы, причиняющие ущерб без видимых причин, и д) наркоманы (компьютерные «ботаники»), аддиктированные по отношению к хакингу[4].

Особое положение среди разновидностей хакинга занимает обретавший популярность на протяжении последнего десятилетия хактивизм[5]. Хактивизм привнес в субкультуру хакеров политическую мотивацию, привлек внимание общественности к проблемам, связанным

[1] Комлев Ю. Ю. Девиантность и преступность в эпоху high-tech, консьюмеризма и глэм-капитализма // Вестник Казанского юридического института МВД России. 2018. Т. 9. № 1. С. 31.

[2] Клаберов продолжают выделять по сей день, что, впрочем, не кажется оправданным, поскольку компьютерные клубы в развитых странах сегодня являются большой редкостью.

[3] Социальным ролям хакеров посвящено немало исследований, одно из них: Масленченко С. В. Социальные роли субкультуры хакеров // Известия Российского государственного педагогического университета имени А. И. Герцена. 2008. № 61. С. 173–176.

[4] О настоящей типологии high-tech-девиантов см.: Комлев Ю. Ю. Указ. соч. С. 32.

[5] Термин hacktivism – «слово-бумажник», результат контаминации (слияния) слов hacker и activism.

с чрезмерной концентрацией власти в руках государств, воспользовавшихся плодами виртуализации. Наиболее показательным является кейс Джулиана Ассанжа и WikiLeaks[1]. После обвинения Дж. Ассанжа в совершении киберпреступления «поднялся глобальный хактивистский бунт. Тогда тысячи хакеров, да и обычных пользователей со всего мира, объединили свои усилия, чтобы отомстить властям США и ряда других стран за давление на WikiLeaks»[2]. Ведущую роль в бунте сыграло децентрализованное хактивистское сообщество Anonymous, деятельность которого не была успешной, но способствовала массовости протеста. Киберпреступность в части хактивизма, таким образом, представляется исключительным явлением, поскольку хактивизм, в полном соответствии с конструктивистской дефиницией преступности[3], не может считаться ничем иным, кроме как преступлением, однако, получает широкое одобрение со стороны общества, ставя под сомнение монополию государства на определение преступности и знаменуя конец сложившегося после теракта 11 сентября 2001 года консенсуса безопасности, вследствие которого американское государство получило возможность неограниченного контроля посредством централизации обращения цифровых данных.

Таковы тенденции развития субкультуры хакеров. Не исключено, что она стоит на пороге пятого этапа своей истории, предполагающего способность каждого пользователя мирового киберпространства стать хакером. Подобный вызов требует разработки новых подходов к противодействию киберпреступности. Сегодня по-прежнему широко применяется метод компьютерного наблюдения: «отслеживается трафик данных, поступающий в компьютер или сеть и выходящий из нее. Другие методы включают скрытую установку программного обеспечения,

---

[1] «По данным американской прокуратуры, основатель WikiLeaks предположительно в 2009 году вступил в сговор с аналитиком Вооруженных сил США Бредли Мэннингом <…>. Ассанж якобы подстрекал Мэннинга к передаче засекреченной информации, которая была использована в ущерб национальной безопасности Соединенных Штатов или в пользу иностранного государства. <…> В результате утечки данных Ассанж, как утверждают американские власти, получил доступ к десяткам и сотням тысяч отчетов о событиях в Афганистане, Ираке, аналитическим запискам о заключенных в Гуантанамо и документации Госдепартамента США». См.: Уголовное преследование руководителя WikiLeaks Джулиана Ассанжа // Российское агентство правовой и судебной информации: сайт. 2020. URL: http://rapsinews.ru/trend/wikileaks_01122010/ (дата обращения: 15.01.2021).

[2] Овчинский В. С. Указ. соч. С. 195.

[3] «Преступность почти полностью конструируется контролирующими институтами, которые устанавливают нормы и приписывают поступкам определенные значения». См.: Гилинский Я. И. Человеческое, слишком человеческое. Алетейя, 2020. С. 64.

предоставляющего информацию о действиях пользователя, внедрение устройств, регистрирующих нажатие клавиш, способных передавать его последовательность в любое место, и размещение скрытых камер, используемых для фиксации комбинаций клавиш и изображения на мониторе»[1]. Предпринимаются попытки создать более эффективные инструменты противодействия. «Начиная с 2017 года, ФБР совместно с компанией For All Secure и университетом штата Пенсильвания приступило к разработке системы искусственного интеллекта Mayhem – первой в мире системы искусственного интеллекта, основными функциями которой являются распознавание индивидуального почерка хакеров и хакерских группировок, а также обнаружение [их] атак»[2]. Криминологам же только предстоит в полной мере осмыслить и исследовать киберпреступность как проявление кибердевиантности и предложить способы разрешения противоречий, лежащих в их основе.

Список литературы

1. Гилинский Я. И. Человеческое, слишком человеческое. Алетейя, 2020.
2. Десятый Конгресс Организации Объединенных Наций по предупреждению преступности и обращению с правонарушителями. Сборник документов / Сост. А. Г. Волеводз. М.: Юрлитинформ, 2001.
3. Дремлюга Р. И. Субкультура хакеров и другие факторы компьютерной преступности // Криминологический журнал Байкальского государственного университета экономики и права. 2008. № 4. С. 22–26.
4. Комлев Ю. Ю. Девиантность и преступность в эпоху high-tech, консьюмеризма и глэм-капитализма // Вестник Казанского юридического института МВД России. 2018. Т. 9. № 1. С. 23–34.
5. Масленченко С. В. Социальные роли субкультуры хакеров // Известия Российского государственного педагогического университета имени А. И. Герцена. 2008. № 61. С. 173–176.
6. Метамодернизм: историчность, аффект и глубина после постмодернизма / Р. ван ден Аккер: [пер. с англ. В. М. Липки; вступит. ст. А. В. Павлова]. М.: РИПОЛ классик, 2020.
7. Овчинский В. С. Криминология цифрового мира: учебник для магистратуры. М.: Норма: ИНФРА-М, 2018.
8. Овчинский В. С. Технологии будущего против криминала. М.: Книжный мир, 2017.
9. Уголовное преследование руководителя WikiLeaks Джулиана Ассанжа // Российское агентство правовой и судебной информации: сайт. 2020. URL: http://rapsinews.ru/trend/wikileaks_01122010/ (дата обращения: 15.01.2021).
10. Barak G. Criminology: an integrated approach. Lanham, Md.: Rowman & Littlefield, 2009.

[1] Barak G. Criminology: an integrated approach. Lanham, Md.: Rowman & Littlefield, 2009. P 105.

[2] Овчинский В. С. Технологии будущего против криминала. М.: Книжный мир, 2017. С. 20.

Е. В. Брадул

КИБЕРТЕРРОРИЗМ: ПРОБЛЕМНЫЕ ВОПРОСЫ ТОЛКОВАНИЯ И КВАЛИФИКАЦИИ

Аннотация: Данная статья посвящена исследованию проблемы кибертерроризма, выявлению специфики данного преступления, а также рассмотрению вопросов толкования и квалификации кибертерроризма.

Ключевые слова: кибертерроризм, кибератака, информационная война, информационный криминал.

CYBER TERRORISM: PROBLEMATIC ISSUES OF INTERPRETATION AND QUALIFICATIONS

Abstract: This article is devoted to researching the problem of cyber terrorism, identifying the specifics of this crime, as well as considering the issues of interpretation and qualification of cyber terrorism.

Keywords: cyberterrorism, cyberattack, information war, information crime.

Научно-технический прогресс, связанный с бурным развитием и внедрением широкого спектра информационно-коммуникационных технологий во все сферы жизни общества, имел как положительные, так и негативные последствия. Отрицательное последствие глобализации информационных процессов и появления глобальных компьютерных сетей проявилось в том, что возможность использования технологических инноваций и изменений стала весьма привлекательной для современных террористов, поскольку использование виртуального пространства (киберпространства) значительно облегчило планирование и осуществление террористических акций, достижение деструктивных, преступных и антисоциальных целей дестабилизации общественного порядка и международной обстановки.

Уязвимыми объектами для кибертеррористических атак стали электростанции и телекоммуникации, правительственные информационные объекты, военные объекты управления, центры управления воздушным движением[1].

Это обуславливает необходимость выработки мировым сообществом действенных методов борьбы с террористическими актами, совершаемыми в киберпространстве.

Данное явление в середине 1980-х годов получило название кибертерроризма (по Б. Колину)[2].

[1] Rouse M. Definition Cyberterrorism. May, 2019. URL: https://searchsecurity.techtarget.com/definition/cyberterrorism (дата обращения: 12.01.2021).

[2] Туронок С. Г. Информационный терроризм: выработка стратегии противодействия // Общественные науки и современность. 2011. № 4. С. 132.

Сегодня продолжает оставаться актуальной проблема наиболее точного выделения специфики данного киберпреступного явления и его отличительных признаков от информационной войны и информационного криминала.

Следует обратить внимание на тот факт, что в науке международного права не выработано единого и устоявшегося толкования понятия кибертерроризма[1].

Американский специалист в области киберпрестпуности и кибербезопасности Д. Деннинг под кибертерроризмом понимает противоправную атаку или угрозу атаки на компьютеры, сети или информацию, находящуюся в них, осуществляемые для причинения максимального ущерба жизненно важным объектам информационной инфраструктуры[2].

По мнению Ю. Бочарова, кибертерроризм является одним из видов традиционного терроризма, имеющим своей целью запугивание и иное воздействие на принятие решений различных структур, используя при этом достижения науки и техники в области компьютерных и информационных технологий и т. п. [3]

Отметим, что характерными особенностями кибертерроризма являются открытость и широкий общественный резонанс террористических актов и выдвигаемых условий. Это обстоятельство служит отличием тактики использования информационного оружия террористами от той, что присуща информационной войне или методам информационного криминала[4]. Также к основным признакам кибертерроризма следует отнести высокую латентность, причинение огромного материального ущерба при незначительных денежных затратах, трансграничный характер, предполагающий нахождение преступников и их жертв в различных государствах.

Для совершения кибертерактов преступники используют различные техники и приемы, такие как создание и включение вирусов в уязвимые сети, хищение и уничтожение информационных ресурсов

---

[1] Маслакова Е. А. Кибертерроризм как новая форма терроризма // Наука и практика. 2015. № 2 (63). С. 80.

[2] Denning D. E. Activism, Hacktivism, and Cyberterrorism: the Internet As a Tool for Influencing Foreign Policy // A revised version appeared in The Computer Security Journal. 2000. Vol. XVI, № 3. P. 15–35.

[3] См.: Соколова О. А. Кибертерроризм: понятие и меры борьбы // Вестник молодых ученых и специалистов Самарского государственного университета. 2017. № 1 (10). С. 114.

[4] См.: Туронок С. Г. Информационный терроризм: выработка стратегии противодействия // Общественные науки и современность. 2011. № 4. С. 132.

с киберпространств, имеющих стратегическую ценность, создание угрозы опубликования секретной информации, распространение дезинформации, а также материалов экстремистской направленности путем захвата веб-сайтов и других каналов средств массовой информации, запуски атаки типа «отказ в обслуживании» и / или создание террористических угроз в электронном виде. Данные приемы постоянно совершенствуются[1].

Кибертеррористы атакуют критически важные системы инфраструктуры, с тем чтобы вывести из строя водоочистные сооружения, вызвать отключение электроэнергии в регионе или нарушить работу трубопровода, нефтеперерабатывающего завода или гидроразрыва пласта. Этот тип кибератак может разрушить крупные города, вызвать кризис общественного здравоохранения, поставить под угрозу общественную безопасность миллионов людей, а также вызвать массовую панику и гибель людей[2].

В апреле 2020 года в результате зарубежной DDoS-атаки на сайт мэрии Москвы (mos.ru) образовались серьезные перебои при оформлении электронных пропусков жителей столицы, необходимых для передвижения по городу. Специалистами был сделан вывод о том, что данные действия были совершены с целью завладения персональными данными жителей или же для дезорганизации работы мэрии[3].

Однако в настоящее время между правительствами различных стран и сообществом информационной безопасности нет консенсуса относительно того, что квалифицируется как акт кибертерроризма. Заметим также, что в современном законодательстве Российской Федерации не закреплено понятие кибертерроризма.

Из-за отсутствия научно обоснованного и юридически проверенного термина ФБР предложило следующее определение: «кибертерроризм – это преднамеренное, политически мотивированное нападение террористических групп и их секретных агентов на компьютерные системы, информацию, программное обеспечение и хранящиеся в них данные, которые приводят к насильственным действиям против гражданских объектов»[4]. Такой подход разделяют большинство аналитиков.

---

[1] См.: Шогенов Т. М. Терроризм в условиях глобализации. Кибертерроризм // Социально-политические науки. 2018. № 3. С. 182.

[2] Rouse M. Op. cit. URL: https://searchsecurity.techtarget.com/definition/cyberterrorism (дата обращения: 12.01.2021).

[3] Жаворонкова Н. Г., Шпаковский Ю. Г. Правовое регулирование противодействия кибертерроризму // Юридическая наука в Китае и России. 2020. № 3. С. 161.

[4] См.: Sobolnikov V. V., Sobolnikova E. V., Sidorova I. A. Cyberterrorism: categorical analysis and psychological criminological problems of counteract. Science and world. 2018. № 5 (57). Vol. II. P. 58.

Однако определить и доказать террористические намерения – довольно сложная задача в ходе расследования подобных нападений в связи с тем, что личность преступников и их цели могут оставаться неизвестными долгое время[1].

На сегодняшний день в юридической науке не утихают споры о включении в Уголовный кодекс РФ специального состава – кибертерроризма.

И. Г. Чекунов, Е. С. Саломатина, Е. Н. Молодчая и др. убеждены, что статья 205 УК РФ нуждается в дополнении частью 2, которая должна предусмотреть ответственность за террористический акт с помощью незаконного проникновения в компьютерные сети. Другие же считают подобное включение излишним, ссылаясь на Пленум Верховного Суда РФ от 09.02.2012 № 1, который позволяет рассматривать в качестве иных действий (ст. 205 УК РФ) и те, что совершаются в киберпространстве[2].

Сходной позиции придерживаются и зарубежные законодатели. Однако стоит отметить тот факт, что некоторые государства все-таки попытались применить уголовно-правовые меры в борьбе с кибертерроризмом. Например, ст. 270-quinquies УК Италии установила ответственность за обучение террористической деятельности с использованием информационных технологий. Ст. 421-2-5-2 УК Франции предусматривает ответственность за распространение информационных материалов, демонстрирующих принадлежность к какой-либо террористической идеологии при этом намеренность лишения жизни[3].

Спорным является вопрос об отнесении к кибертерроризму действий террористов, совершаемых в сети Интернет с целью популяризации и осуществления своей деятельности, но не для непосредственного совершения террористических актов, проявляющихся в виде финансовых сборов для поддержки террористических организаций, собирания информации об объектах критической инфраструктуры, оказания психического воздействия и вербовки граждан с помощью интернет-ресурсов. По мнению ряда исследователей, квалифицировать

[1] См.: Ивашкевич И. С. Международное сотрудничество в борьбе с кибертерроризмом // Концепции современного образования: вопросы продуктивного взаимодействия наук в рамках технического прогресса. 2020. С. 106.

[2] См.: Кулешова Г. П., Капитонова Е. А., Романовский Г. Б. Правовые основы противодействия кибертерроризму в России и за рубежом с позиции общественно-политического измерения // Всероссийский криминологический журнал. 2020. Т. 14. № 1. С. 158.

[3] Там же.

подобные действия как терроризм не верно, поскольку они не соответствуют всем признакам состава преступления, предусмотренного ст. 205 УК РФ.

Очевидно, что сегодня назрела крайняя необходимость в принятии нормативных актов, которые должны установить единый подход к толкованию таких понятий, как «киберпреступление» и «кибертерроризм», а также основные механизмы предупреждения и расследования преступлений, совершенных в виртуальном пространстве.

Список литературы

1. Жаворонкова Н. Г., Шпаковский Ю. Г. Правовое регулирование противодействия кибертерроризму // Юридическая наука в Китае и России. 2020. № 3. С. 160–166.
2. Ивашкевич И. С. Международное сотрудничество в борьбе с кибертерроризмом // Концепции современного образования: вопросы продуктивного взаимодействия наук в рамках технического прогресса. 2020. С. 103–107.
3. Кулешова Г. П., Капитонова Е. А., Романовский Г. Б. Правовые основы противодействия кибертерроризму в России и за рубежем с позиции общественно-политического измерения // Всероссийский криминологический журнал. 2020. Т. 14. № 1. С. 156–165.
4. Маслакова Е. А. Кибертерроризм как новая форма терроризма // Наука и практика. 2015. № 2 (63). С. 79–81.
5. Соколова О. А. Кибертерроризм: понятие и меры борьбы // Вестник молодых ученых и специалистов Самарского государственного университета. 2017. № 1 (10). С. 114–116.
6. Туронок С. Г. Информационный терроризм: выработка стратегии противодействия // Общественные науки и современность. 2011. № 4. С. 131–140.
7. Шогенов Т. М. Терроризм в условиях глобализации. Кибертерроризм // Социально-политические науки. 2018. № 3. С. 181–182.
8. Denning D. E. Activism, Hacktivism, and Cyberterrorism: the Internet As a Tool for Influencing Foreign Policy // A revised version appeared in The Computer Security Journal. 2000. Vol. XVI, № 3. P. 15–35.
9. Rouse M. Definition Cyberterrorism. May, 2019. URL: https://searchsecurity.techtarget.com/definition/cyberterrorism (дата обращения: 12.01.2021).
10. Sobolnikov V. V., Sobolnikova E. V., Sidorova I. A. Cyberterrorism: categorical analysis and psychological criminological problems of counteract. Science and world. 2018. № 5 (57). Vol. II. P. 57–60.

Т. О. Брылева

ОСНОВОПОЛАГАЮЩИЕ ПРИНЦИПЫ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПНОСТИ В РОССИЙСКОЙ ФЕДЕРАЦИИ

Аннотация: В статье автор выделил основополагающие принципы противодействия киберпреступности в Российской Федерации, которые, по его мнению, необходимо закрепить в законодательстве.

Ключевые слова: киберпреступность, принципы противодействия киберпреступности, законодательное регулирование.

FUNDAMENTAL PRINCIPLES OF COUNTERING CYBERCRIME IN THE RUSSIAN FEDERATION

Abstract: In the article, the author identifies the fundamental principles of countering cybercrime in the Russian Federation, which, in his opinion, should be enshrined in legislation.

Keywords: cybercrime, principles of countering cybercrime, legislative regulation.

Рассматривая киберпреступность в целом, можно сказать, что это совокупность преступлений, совершаемых посредством использования интернет-технологий. В законодательных актах точного определения киберпреступности не закреплено, дается лишь отсылка на синонимичный термин, например, «компьютерные преступления», «преступления в сфере высоких технологий».

Поскольку количество постоянных пользователей сети Интернет растет, увеличивается и число преступлений, совершаемых дистанционно. Прежде всего этому способствуют анонимность пользователей, сложность раскрытия киберпреступлений, правовые пробелы. Нельзя не отметить и влияние психологического фактора – в рамках киберпространства человек может совершать действия, на которые не решился бы в реальном мире. Широкое использование социальных сетей также приводит к появлению новых способов совершения правонарушений.

В Российской Федерации законодательство в области киберпространства находится лишь на стадии становления. Данное положение обусловлено тем, что широкое применение информационных технологий в России и соответственно увеличение количества с ними связанных правонарушений возникли сравнительно недавно. Несмотря на то, что активное формирование нормативной базы началось в 90-е годы,

к 1997 году еще не была сформирована эффективная система защиты информационных отношений, так как недоставало соответствующих правовых механизмов. Для сравнения – в Японии уже к 1985 году был принят Закон о размещении интегральных полупроводниковых схем, в документе предусматривались наказания, цель которых заключалась в охране информации.

Несмотря на то, что вопрос о противодействии киберпреступлениям стоит на международном уровне, каждая из стран занимается разработкой собственной стратегии, позволяющей решить проблему на внутригосударственном уровне. Особую роль в координации действий государств сыграла «Большая восьмерка». На одном из заседаний было принято решение о более тесном сотрудничестве правоохранительных органов стран-участниц. Была создана «Лионская группа», основной целью которой была борьба с киберпреступностью[1]. Стоит отметить, что объединение усилий России с другими государствами очень важно для создания нормативной базы в сфере противодействия киберпреступности и будет максимально результативным, если проводить анализ опыта других стран, постараться спрогнозировать развитие появления новых видов киберугроз, сделать акцент на выработку мер профилактики.

Для нашей страны изучение законодательства о кибербезопасности в странах Европы и Азии является весьма актуальным.

В частности, интересен опыт Японии, где разработка первых нормативно-правовых актов, регулирующих отношения в сфере информационной безопасности, началась с прошлого века. В 2001 году был принят закон, в соответствии с которым в Уголовный кодекс были внесены изменения, касающиеся установления уголовной ответственности за новые виды компьютерных преступлений[2]. В 2018 году в Токио открыли единый центр борьбы с киберпреступностью.

Стоит проанализировать и опыт Китая. В этом государстве первый документ, регулирующий правоотношения в сфере киберпреступности, был принят еще в 1999 году. Значительное внимание в нем уделяется такому элементу, как шифрование данных. В 2015 году был принят закон

---

[1] См.: Сухаренко А. Н. Современные криминальные вызовы и угрозы информационной безопасности России. URL: http://sartraccc.ru/Press/special/contr_terror_1_12.pdf (дата обращения: 16.01.2021).

[2] См.: Морозов Н. А. Киберпреступность в Японии в XXI веке // Азиатско-тихоокеанский регион: экономика, политика, право. Владивосток, 2014. № 3–4. С. 100–109.

о национальной безопасности. Положения распространяют свое действие на достаточно широкий круг лиц, а также обозначают важность укрепления суверенитета киберпространства в Китае. С 2020 года были введены новые правила кибербезопасности, основными целями которых являются создание безопасного киберпространства, обеспечение национальной безопасности.

Законодательство, регламентирующее противодействие киберпреступлениям, активно развивается и в других странах. Например, в США впервые за 15 лет была принята новая стратегия кибербезопасности. Документ предписывает федеральному правительству предпринимать действия для обеспечения долгосрочного улучшения состояния безопасности в киберпространстве для всех американцев.

Следует отметить, что общими направлениями в стратегиях и создании законодательных актов стран признаются защита интересов субъектов правоотношений, обеспечение безопасности информационных систем от несанкционированного доступа.

В законодательствах разных стран, помимо различий, много и схожих положений. Например, практически во всех государствах перечень преступлений в сфере информационной безопасности схож, чаще всего выделяют: компьютерное мошенничество и хищение, коммерческий шпионаж, вымогательство с использованием компьютерной техники.

Учеными и политиками Российской Федерации неоднократно отмечалось, что национальная правовая база в области борьбы с киберпреступностью не совсем совершенна по причине динамичности развития общественных отношений с использованием сети Интернет. Для формирования законодательства необходимы не только юридические, но и специальные знания в сфере использования информационных технологий. Поэтому так важны на стадии разработки законопроектов сотрудничество и учет мнения специалистов в области информационной безопасности.

В Люксембурге и Эстонии предусмотрены даже специальные курсы по борьбе с киберпреступностью для сотрудников правоохранительных органов, а также уделяется большое внимание профилактике посредством информирования граждан о безопасном поведении в киберпространстве[1].

[1] Рудакова Ю. С. Международный опыт в сфере противодействия экономическим преступлениям, совершаемым в киберпространстве // STUDENT RESEARCH: сборник статей VI Международного научно-практического конкурса. Изд-во: Наука и Просвещение (ИП Гуляев Г. Ю.). Пенза, 2019. С. 161–163.

Таким образом, можно сделать вывод о том, что в Российской Федерации процесс формирования законодательства в сфере противодействия киберпреступлениям должен основываться на следующих основных принципах:

1. Международное сотрудничество;
2. Приоритет профилактики киберпреступлений;
3. Использование международного опыта для прогнозирования появления новых преступлений;
4. Взаимодействие законодателя со специалистами в области информационной безопасности для формирования актуальной правовой базы.

Указанные принципы должны быть выделены не только в теории права, но и закреплены законодательно, что создаст фундамент для принятия актуальных нормативных правовых актов.

Список литературы

1. Рудакова Ю. С. Международный опыт в сфере противодействия экономическим преступлениям, совершаемым в киберпространстве // STUDENT RESEARCH: сборник статей VI Международного научно-практического конкурса. Изд-во: Наука и Просвещение (ИП Гуляев Г. Ю.). Пенза, 2019. С. 161–163.
2. Сухаренко А. Н. Современные криминальные вызовы и угрозы информационной безопасности России. URL: http://sartraccc.ru/Press/special/contr_terror_1_12.pdf (дата обращения: 16.01.2021).
3. Морозов Н. А. Киберпреступность в Японии в XXI веке // Азиатско-тихоокеанский регион: экономика, политика, право. Владивосток, 2014. № 3–4. С. 100–109.

Н. Э. Войнов

КИБЕРПРЕСТУПНОСТЬ В РОССИЙСКОЙ ФЕДЕРАЦИИ: СОВРЕМЕННОЕ СОСТОЯНИЕ И АКТУАЛЬНЫЕ ПРОБЛЕМЫ

Аннотация: В данной научной статье рассматривается некоторый ряд проблем, связанных с деятельностью правоохранительных органов Российской Федерации по выявлению и дальнейшему расследованию преступлений, совершаемых с применением информационно-телекоммуникационных технологий.

Ключевые слова: информационно-телекоммуникационные технологии, компьютерные системы, киберпреступность, преступления в сфере компьютерной информации.

CYBERCRIME IN THE RUSSIAN FEDERATION: CURRENT STATE AND URGENT PROBLEMS

Abstract: This scientific article examines a number of problems that are associated with the activities of the law enforcement agencies of the Russian Federation to identify and further investigate crimes committed with the use of information and telecommunication technologies.

Key words: information and telecommunication technologies, computer systems, cybercrime, crimes in the field of computer information.

Со вступлением всего мирового сообщества в новую эпоху информационных технологий невозможно представить жизнь человека без использования достижений технического и научного прогресса. Всеобщая компьютеризация и информатизация населения способствуют качественному и быстрому решению повседневных задач, а также достижению определенных целей.

К несчастью, технические инновации используются не только в качестве вспомогательных элементов жизни человека, но и для совершения противоправных деяний посредством создания различных вирусов, которые могут нанести вред компьютерной информации, а также осуществления кибератак на информационно-телекоммуникационные сети.

Стоит отметить, что количество преступлений, совершенных с использованием информационных технологий, с каждым годом набирает все большие и большие обороты, которые отрицательно сказываются на жизни не только граждан отдельного государства, но и всего мира.

Необходимо обратиться к официальной статистике Министерства внутренних дел Российской Федерации, которая показывает, что

за январь–ноябрь 2019 года посредством применения информационно-телекоммуникационных технологий было совершено 157 306 противоправных деяний, а за аналогичный период 2018 года – 814 301. Это свидетельствует о том, что всего лишь за один год доля преступлений, совершаемых с применением информационно-телекоммуникационных технологий, выросла почти наполовину[1].

По данным Генеральной прокуратуры Российской Федерации, в 2020 году количество преступлений в сфере компьютеризации и информатизации увеличилось с 66 945 до 91 567. Это говорит о том, что доля совершенных преступных деяний с применением информационно-телекоммуникационных технологий составляет 4,5 % от общего числа всех зарегистрированных преступлений в Российской Федерации, а это в свою очередь каждое 20-е преступление[2].

Анализируя судебную, а также следственную практику, стоит отметить, что наиболее распространенными преступлениями с применением информационно-телекоммуникационных технологий являются: создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ); неправомерный доступ к компьютерной информации (ст. 272 УК РФ); мошеннические действия, совершенные с использованием электронных средств платежа (ст. 159.3 УК РФ). Следует подчеркнуть, что мошенничество с использованием платежных (банковских) карт (ст. 159.3 УК РФ) в 2020 году выросло в 8 раз по сравнению с аналогичными преступлениями, предусмотренными главой 28 УК РФ.

Представленные данные оставляют желать лучшего, тем более что раскрываемость преступлений в сфере информационно-телекоммуникационных технологий ежегодно варьируется от 44 до 49 %.

Поэтому стоит сказать о необходимости разработки качественных методик по организации раскрытия и дальнейшего расследования преступлений, совершаемых с применением информационно-телекоммуникационных технологий. Для достижения поставленных целей необходимо непосредственное участие со стороны правоохранительных органов и государства, которые смогут надлежащим образом организовать процесс по выявлению и раскрытию противоправных деяний, а также привлечь квалифицированных специалистов в этой области.

---

[1] Официальный сайт Министерства внутренних дел РФ. URL: http://mvd.ru/presscenter/statistics/reports/item/804701 (дата обращения: 15.01.2021).

[2] Официальный сайт Генеральной прокуратуры Российской Федерации. URL: https://genproc.gov.ru (дата обращения: 15.01.2021).

В июле 2018 года на Международном конгрессе по кибербезопасности Президент Российской Федерации В. В. Путин озвучил ряд мер, которые направлены на осуществление кибербезопасности страны. В данный список вошли: международное сотрудничество, использование отечественного программного обеспечения, а также подготовка квалифицированных кадров, создание системы обмена информацией о кибератаках[1].

Принятие данных мер Правительством Российской Федерации позволит избежать множественных атак со стороны киберпреступников, а также укрепить взаимоотношения с иностранными коллегами. Не стоит забывать и о том, что это также позволит обмениваться опытом для дальнейшей защиты информационно-телекоммуникационных сетей.

В качестве примера можно привести созданный вирус Petya, который стал угрозой мирового масштаба в 2017 году. Его принцип действия заключался в том, что Petya полностью блокировал операционную систему и в последующем требовал выкуп в размере 300 долларов в «биткоинах». От его деятельности пострадали такие крупные компании, как Хоумкредит, Роснефть, Сбербанк, Башнефть[2].

Для того чтобы предотвратить, а также восстановить ущерб, нанесенный вирусом Petya, потребовалось немало времени. Для этого были привлечены квалифицированные эксперты-криминалисты в сфере информационных технологий, а также сотрудники «Лаборатории Касперского».

По данным из разных источников известно, что эта программа нанесла ущерб более чем 60 странам мира.

После изучения нынешнего состояния информационно-телекоммуникационного пространства, научной литературы, а также в результате анализа сведений о состоянии преступности и технической оснащенности правоохранительных органов Российской Федерации, стоит выделить ряд проблем, которые требуют решения:

1. Деятельность по раскрытию и расследованию преступлений по борьбе с киберпреступностью основывается на принципах, которые по большей части уже неэффективны: на данный момент правоохранительные органы с имеющимися техническими средствами не всегда могут противопоставить себя «новой преступности»;

---

[1] См.: Пленарное заседание Международного конгресса по кибербезопасности. URL: http://kremlin.ru/events/president/ news/57957 (дата обращения: 15.01.2021).

[2] См.: Вирус Petya. URL: ru.wikipedia.org›wiki/Petya. (дата обращения: 15.01.2021).

2. Не полностью урегулирована система государственных учреждений, которая проводит компьютерно-технические и иные экспертизы по делам о преступлениях с применением информационно-телекоммуникационных технологий;
3. Не полностью сформированы предмет, метод, цели и задачи цифровой криминалистики; данное направление требует осознания и развития практических рекомендаций по работе с электронными, виртуальными, цифровыми следами, программным обеспечением и интернет-сервисами;
4. Недостаточно развито законодательство в сфере противодействия киберпреступлениям (например, в УК РФ не установлена уголовная ответственность за социальную инженерию, а также за распространение спама)[1].

Подводя итоги вышесказанного, стоит отметить, что для эффективной реализации борьбы с киберпреступностью необходимо непосредственное участие государства, которое смогло бы надлежащим образом разрабатывать программы в сфере защиты информационно-телекоммуникационных технологий, а также проводить кадровую политику для дальнейшего формирования грамотного уровня специалистов.

Также необходимо сделать акцент на том, что страны мира должны объединиться для совместной борьбы с киберпреступностью. Это позволит заимствовать некий опыт, который даст толчок развитию в сфере компьютеризации информатизации для других стран.

Список литературы

1. Вирус Petya. URL: ru.wikipedia.org›wiki/Petya. (дата обращения: 15.01.2021).
2. Гаврилин Ю. В. Преступления в сфере компьютерной информации: квалификация и доказывание: учебное пособие. М.: ЮИ МВД РФ, 2019.
3. Официальный сайт Министерства внутренних дел Российской Федерации. URL: http://mvd.ru/ presscenter/statistics/reports/item/804701 (дата обращения: 15.01.2021).
4. Официальный сайт Генеральной прокуратуры Российской Федерации. URL: https://genproc.gov.ru (дата обращения: 15.01.2021).
5. Пленарное заседание Международного конгресса по кибербезопасности. URL: http://kremlin.ru/events/president/ news/57957 (дата обращения: 15.01.2021).
6. Расширенное заседание коллегии Министерства внутренних дел от 26.02.2020. URL: http: https://мвд.рф/news/item/19641761 (дата обращения: 15.02.2021).
7. Торопина Т. Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы: дис. ... канд. юрид. наук. Владивосток. 2020.

[1] Гаврилин Ю. В. Преступления в сфере компьютерной информации: квалификация и доказывание: учебное пособие. М.: ЮИ МВД РФ, 2019.

О. Д. Воробьева

ФИШИНГ КАК ТИП КИБЕРПРЕСТУПНОСТИ. АКТУАЛЬНЫЕ ПРОБЛЕМЫ ПРИВЛЕЧЕНИЯ К УГОЛОВНОЙ ОТВЕТСТВЕННОСТИ

Аннотация: В статье рассматриваются основные аспекты такой разновидности киберпреступлений, как фишинг: его исторический аспект и проявления в современном мире. Автором рассмотрены цели, виды и способы совершения киберпреступлений. В процессе написания статьи проведен опрос, цель которого – выявить процент пострадавших от фишинга и основные его площадки. Раскрыты актуальные проблемы законодательства, связанного с киберпреступлениями, и предложены пути их решения.

Ключевые слова: фишинг, киберпреступность, социальная инженерия.

PHISHING AS A TYPE OF CYBERCRIME. ACTUAL PROBLEMS OF PROSECUTION

Abstract: The article examines aspects of such a type of cyberprevention as phishing: its historical aspect and manifestations in the modern world. The author considers the goals, types and methods of committing cybercrimes. In the process of writing this article, a survey was conducted to determine the percentage of victims of phishing and its main sites. Revealed topical problems of legislation related to cybercrimes and suggested ways to solve them.

Key words: phishing, cybercrime, social engineering.

В настоящее время, обусловленное эпохой пандемии COVID-19, многие работники, особенно в центральных городах, перешли на дистанционный формат работы и обучения. Вместе с этим мошенники, занимающиеся киберпреступлениями, начали переходить на более высокий и изощренный уровень своих деяний. С каждым днем количество кибератак непрерывно возрастает. 20 ноября официальный представитель МВД России Ирина Волк сообщила о том, что количество киберпреступлений за 2020 год по сравнению с 2019 возросло на 94,6 %1. По статистике каждый 12-й звонок по России – это спам или кибератака.

Согласно отчету, опубликованному Генпрокуратурой РФ, можно проследить, что количество преступлений растет, но при этом их раскрываемость уменьшается. Как отмечает адвокат в сфере киберправа С. Дарбинян, «огромное количество реально совершенных преступлений остается за бортом. Например, ситуации, когда у пользователя

[1] О состоянии преступности по итогам 10 месяцев 2020 года. URL: https://мвд.рф/news/item/21909392/ (дата обращения: 06.01.2021).

угоняют «танчик» (танк в многопользовательской онлайн-игре World of Tanks) ценой в несколько тысяч долларов или с помощью вирусов похищают личные пароли от криптокошельков и уводят затем Etherium или Bitcoin. О таких преступлениях не заявляют, их количество никто не отслеживает, по ним не возбуждаются уголовные дела»1.

В данной статье попробуем разобраться с таким понятием, как «фишинг» в ключе киберпреступности и с тем, как с ним бороться с точки зрения права.

Фишинг – это вид мошенничества, целью которого является получение доступа к конфиденциальной информации пользователя, логину, паролю, счету и т. п. Фишинг считается одним из современных видов мошенничества в Интернете, хотя первые его проявления начались в 1996 году, когда мошенники представлялись сотрудниками компании America Online и, получая данные пользователей, рассылали спам. В Российской Федерации фишинг стал обретать свою популярность в 2007–2009 годах, когда фишеры вышли на уровень социальных сетей, и по оценкам специалистов, более 70 % фишинговых атак прошли успешно.

Остановимся более подробно на вопросе о том, как именно работает данный вид мошенничества. Жертвой мошенничества может стать каждый, это могут быть как работники финансовых учреждений, так и пользователи их услуг. Жертву вводят в заблуждение, представляясь работником той или иной сферы и далее используют различные приемы и способы, для того чтобы жертвы, испытывая страх или иные эмоциональные порывы, добровольно предоставляли фишеру личные данные2. Нередки случаи, когда приходит сообщение из «банка» о том, что со счета пытались снять денежные средства и для того чтобы это предотвратить, необходимо выслать свой номер карты. Под страхом потерять все свои денежные средства на карте, жертвы, зачастую не думая о негативных последствиях, сообщают свои реквизиты. Безусловно, фишинг это мошенничество, однако на сегодняшний день запрет данного вида мошенничества не находит своего закрепления ни в отечественном, ни в зарубежном законодательстве. А тем временем преступники придумывают и совершенствуют все более изощренные модели киберпреступлений. В настоящее время Уголовный кодекс нуждается в серьезных

---

[1] Крипторынок останется вне закона. URL: https://www.advgazeta.ru/mneniya/kriptorynok-ostanetsya-vne-zakona/ (дата обращения: 06.01.2021).

[2] См.: Гайфутдинов Р. Р. К вопросу о типологии личности компьютерных преступников с учетом характера и мотивации их криминальной деятельности // Вопросы российского и международного права. 2017. Т. 7. № 4. С. 245–256.

дополнениях, соответствующих современным реалиям. Еще с 2015 года обсуждался законопроект об уголовной ответственности за фишинг, который с позиции «проекта» до сегодняшнего дня не сдвинулся. Эта проблема в настоящее время является не только актуальной для законодателя, но и актуальной темой научных исследований. Авторы выделяют направления анализа фишинга, особые черты киберпреступников, группы наиболее уязвимых категорий населений1.

Для того чтобы бороться с данной проблемой, очевидным кажется решение подготовки кадров, специализирующихся именно на компьютерных технологиях. В настоящий период приоритетным направлением реформирования являются именно подготовка и обучение специалистов в области противодействия киберкриминалу. Обучение кадров правоохранительных органов должно происходить с учетом специфики киберпреступлений на техническом, физическом, аппаратном, программном и криптографическом уровнях. При подготовке специалистов отдельно следует рассматривать компьютерную криминалистику (форензику), уделять внимание методам сбора цифровых доказательств, изучению программного обеспечения, облегчающего разработку и объединения разных компонентов больших программных проектов (фреймворков) для криминалистического анализа и проведения оперативных исследований на удаленных конечных точках. Бороться с киберпреступностью можно только с помощью методов, которыми пользуются преступники. Методы, которые известны юридической науке на сегодняшний день, считаются не до конца эффективными.

Теперь необходимо подробнее остановиться непосредственно на самой технологии осуществлении фишинга. Способов его осуществления несколько, это могут быть рассылки сообщений, звонки на телефон, с просьбой перевести деньги родственнику, вернуть ошибочно уплаченные деньги, предложения о переоформлении кредита2.

При написании данной статьи был проведен опрос, в котором приняли участие 30 человек различных возрастных групп. В результате данного опроса выяснилось, что 28 опрошенных подвергались фишингу. Из них 19 – переводили денежные средства и сообщали реквизиты мошенникам. То есть 63 процента мошеннических действий были успешными. Один

[1] См.: Бородкина Т. Н., Павлюк А. В. Киберпреступления: понятие, содержание и меры противодействия // Социально-политические науки. 2018. № 1. С. 135–137.

[2] См.: Могунова М. М. Технология осуществления и правовая регламентация незаконного овладения персональными банковскими данными (фишинг) // Вестник Саратовской государственной юридической академии. 2020. С. 135–141.

из опрошенных поделился своей историей: «Примерно в июне 2020 года мне позвонил телефонный номер, который выглядел как телефон компании. Обычно я не беру незнакомые номера, но почему-то именно этот звонок мне показался интересным, я взял трубку. На другой стороне провода мужчина представился как «В.», сотрудник Сбербанка, и сообщил о том, что у них отобразились подозрительные операции с моей банковской картой, будто кто-то в Тюмени пытался списать 3 тысячи, 5 тысяч. Я, конечно, испугался и спросил, что с этим можно сделать, на что мне предложили заблокировать временно операции по карте. Для этого необходимо назвать номер карты и три цифры с оборотной стороны. Когда я начал сомневаться в честности звонившего мне сотрудника, я сказал, что у меня нет с собой карты, а номер наизусть я не помню, после чего от него последовала агрессия и угрозы». Также большое количество опрошенных столкнулись с фишингом, покупая билеты на железнодорожные поезда или заказывая доставку с известных сайтов.

Наиболее серьезной проблемой фишинга является добровольный характер поведения жертвы. Из-за того, что преступник обладает набором психологических приемов и способов, жертва, находясь под его воздействием, добровольно сообщает персональные данные или переводит деньги. Данные приемы уже используются не только в отношении обычных граждан, но и в отношении лиц, которые в силу своих должностных полномочий обладают рядом конфиденциальной информации1.

Сложностью в борьбе с фишингом является то, что преступники редко пользуются одним и тем же способом, то есть изначально проходит волна одного метода, и когда люди уже готовы к тому, что такое может произойти, их тактика кардинально меняется. Важной особенностью является дистанционный характер данного преступления. Невозможно выйти на личный контакт, узнать имя мошенника, его местонахождение, невозможно выследить его по адресам и реквизитам2. Фишинг может быть как почтовым – в виде рассылки по электронным адресам, онлайновым – в виде копирования известных сайтов, с изменением буквально одной буквы в адресе страницы, так и комбинированным – сочетающим в себе несколько способов.

Что касается ответственности, то видится необходимым ввести уголовную ответственность за фишинг в финансовой сфере, так как существующий пробел ведет к тому, что субъекты экономических отношений несут огромные убытки, а преступления в свою очередь нарастают

[1] См.: Могунова М .М. Указ. соч. С. 135–141.

[2] См.: Тулегенов В. В. Киберпреступность как форма выражения криминального профессионализма // Криминология вчера, сегодня, завтра. 2014. № 2. С. 94–97.

и мутируют. Предлагается переформулировать статью 272.1 УК РФ, изменив формулировку «неправомерный доступ к охраняемой законом компьютерной информации» на «получение путем введения в заблуждение или методов социальной инженерии», поскольку неправомерным доступом является незаконное либо не разрешенное собственником или иным ее законным владельцем использование возможности получения компьютерной информации, однако, как было отмечено выше, мошенники обладают рядом психологических приемов, которые позволяют им получить согласие собственника, путем введения его в заблуждение.

Вторым немаловажным способом являются обучение сотрудников правоохранительных органов, внедрение в программы обучения и переподготовки кадров таких предметов, как «социальная инженерия», «основы борьбы с киберпреступностью», «правовые основы информационной безопасности» и других.

И наиболее простым и малозатратным из способов является просвещение населения. Ведь если в СМИ, на многих рекламных щитах, в школах, университетах, Интернете, государственных учреждениях будет напоминание о необходимости с осторожностью относиться к получаемым интернет-рассылкам, о том, что нельзя поддаваться на открытые угрозы, когда речь идет о получении конфиденциальной информации, и о необходимости остерегаться общих формулировок в запросах, то процент жертв киберпреступлений явно станет меньше.

Список литературы

1. Бородкина Т. Н., Павлюк А. В. Киберпреступления: понятие, содержание и меры противодействия // Социально-политические науки. 2018. № 1. С. 135–137.
2. Гайфутдинов Р. Р. К вопросу о типологии личности компьютерных преступников с учетом характера и мотивации их криминальной деятельности // Вопросы российского и международного права. 2017. Т. 7. № 4. С. 245–256.
3. Кочкина Э. Л. Определение понятия «киберпреступление». Отдельные виды киберпреступлений // Сибирские уголовно-процессуальные и криминалистические чтения. 2017. № 3. С. 49–53.
4. Крипторынок останется вне закона. URL: https://www.advgazeta.ru/mneniya/kriptorynok-ostanetsya-vne-zakona/ (дата обращения: 06.01.2021).
5. Могунова М. М. Технология осуществления и правовая регламентация незаконного овладения персональными банковскими данными (фишинг) // Вестник Саратовской государственной юридической академии. 2020. С. 135–141.
6. О состоянии преступности по итогам 10 месяцев 2020 года. URL: https://мвд.рф/news/item/21909392/ (дата обращения: 06.01.2021).
7. Тулегенов В. В. Киберпреступность как форма выражения криминального профессионализма // Криминология вчера, сегодня, завтра. 2014. № 2. С. 94–97.

С. Д. Ганюшкина

КАЗИНО В СЕТИ ИНТЕРНЕТ КАК ОТДЕЛЬНЫЙ ВИД КИБЕРПРЕСТУПНОСТИ: НЕВИДИМАЯ УГРОЗА

Аннотация: Автор анализирует угрозы, возникающие с распространением в сети Интернет нелегальных онлайн-казино. Предлагаются меры по предупреждению таких преступлений.

Ключевые слова: онлайн-казино, киберпреступность, предупреждение преступности.

INTERNET-CASINOS AS A SEPARATE TYPE OF CYBERCRIME: AN INVISIBLE THREAT

Abstract: The author analyzes the threats that arise from the spread of illegal online casinos on the Internet. Also, measures are proposed to prevent such crimes.

Keywords: online casino, cybercrime, crime prevention.

Преступность в целом – явление больше социальное, так как непременно связанно с поведением людей, их мыслями, чувствами. Одно из самых опасных чувств – азарт. Чувство предвосхищения успеха, возникающее наиболее часто во время игры (осмысленной непродуктивной деятельности, важность которой заключается не в результате, а в самом процессе), связанной со случаем или риском. У азарта есть два важнейших признака:

1. В состоянии азарта эмоциональная сфера доминирует над волевой и интеллектуальной.
2. Деятельность, осуществляемая под влиянием азарта, всегда направлена на удовлетворение той потребности, которую человек считает для себя актуальной[1].

Как показывает исследование, проведенное специалистами Государственного научного центра социальной и судебной психиатрии имени В. П. Сербского, избавиться от тяги к игре гораздо сложнее, чем от наркомании. При этом риск стать игроманом зависит больше от характера и темперамента, чем от социальных параметров. Тяжесть игромании не зависит от интеллектуальности игры: то есть страсть к преферансу не менее страшна, чем страсть к рулетке[2].

---

[1] См: Севостьянов Р. А., Просвирин Е. В. Проблемы уголовно-правового регулирования организации и ведения незаконного игорного бизнеса: монография. М.: Юрлитинформ, 2013. 208 с.

[2] См.: Паевский А. Доиграться до психушки: российские ученые озаботились проблемой игромании // Газета.ru. URL: https://www.gazeta.ru/science/2006/06/21_a_679541.shtml?lj2 (дата обращения: 12.01.2021).

Очевидно, что, стремясь получить материальную выгоду, преступники не могут упустить возможность сыграть на чувстве азарта людей.

В настоящее время Россия регулирует игорный бизнес следующим образом: согласно Федеральному Закону от 29.12.2006 № 244-ФЗ «О государственном регулировании деятельности по организации и проведению азартных игр и о внесении изменений в некоторые законодательные акты Российской Федерации» в России создаются пять игорных зон. При этом на территории одного субъекта допускается размещение только одной игорный зоны. Перечислим эти субъекты: Республика Крым, Алтайский край, Краснодарский край, Приморский Край, Калининградская область.

Исключительно в этих зонах допускается создание игорных заведений (казино / зал игровых автоматов), исключение составляют букмекерские конторы и тотализаторы. Само казино отличается тем, что азартные игры в нем ведутся с использование игровых столов. Например, в казино наиболее распространенные игры: рулетка, покер, блэк-джек, очко и т. д. Главное отличие зала игровых автоматов (исходя из названия) – наличие специального оборудования, через которое участники играют в азартные игры.

Места игорных зон располагаются в курортных, отдаленных местах. Все без исключения территории находятся на государственной границе. Думается, такое расположение связано с желанием оградить большую часть населения от пагубного влияния азартных игр, оставив при этом возможность насладиться ими в отпуске. Игорный бизнес – высокодоходный как для владельцев казино, его работников, так и для государства, облагающего игорные заведения высоким налогом. Например, согласно ст. 369 НК РФ, налоговая ставка за один игровой стол составляет от 50 до 250 тысяч рублей. Стоит ли говорить, что игровые столы в казино исчисляются десятками.

Но у игорных заведений все еще есть один большой минус – они находятся слишком далеко даже для жителей указанных субъектов. При этом человек, испытавший азарт хоть раз, стремится снова получить эти острые ощущения.

Именно поэтому с развитием новых технологий, сети Интернет, на смену игорным заведениям пришло онлайн-казино (не имеются в виду тотализаторы и букмекерские конторы), деятельность которого в соответствии с п. 3 ст. 5 Закона об организации и проведении азартных игр категорически запрещена.

У онлайн-казино есть ряд своих «преимуществ»:

1. К ним можно получить дистанционный доступ. Игроку не нужно ехать куда-либо, а для игры нужны только выход в Интернет и техническое устройство.
2. Другим игрокам неизвестны настоящие имена соперников, их лица. При этом одновременно играть могут десятки, сотни игроков.
3. Для организаторов таких заведений стартовый капитал на открытие несравнимо меньше, чем у традиционных заведений.
4. Привлечь к ответственности лиц, организовавших онлайн-казино, практически невозможно благодаря анонимности, которая достигается использованием современных технологий.

Перейдем непосредственно к тому, что онлайн-казино являются проявлением киберпреступности. Чтобы это объяснить, следует дать характеристику киберпреступности в целом.

В узком смысле под кибепреступностью понимают любое противозаконное поведение в форме электронных операций, направленное против безопасности компьютерных систем и обрабатываемых ими данных. В широком смысле такие преступления охватывают любое незаконное поведение, осуществляемое с помощью компьютерной системы или сети[1].

Существуют также термины «компьютерная преступность» и «интернет-преступность». Т. Л. Тропинина указывает, что термин «компьютерная преступность» недостаточен для охвата всех деяний, совершаемых с использованием вычислительной техники, глобальных сетей. Киберпреступность же сочетает в себе любые средства доступа к киберпространству[2]. Термином «интернет-преступность» принято называть часть компьютерной преступности. Ее главным критерием является совершение преступлений с использованием или посредством сети Интернет[3].

Можно выделить следующие критерии киберпреступности, являющиеся общими для всех указанных терминов:

1. Высокотехнологический характер, вызванный использованием IT-технологий, информационно-телекоммуникационных сетей, компьютерных устройств и т. п.

---

[1] См.: Агапов П. В. Противодействие киберпреступности в аспекте обеспечения национальной безопасности: монография / Акад. Ген. Прокуратуры Рос. Федерации. М., 2014. С. 11.

[2] См.: Тропинина Т. Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы: дис. … канд. юрид. наук. Владивосток, 2005. С. 36.

[3] См.: Дремлюга Р. И. Интернет-преступность. Владивосток, 2008. С. 44–45.

2. Высокая степень латентности, которая обусловлена различными объективными факторами. Например, незаметностью компьютерных преступлений для большинства населения, сложностью их выявления и расследования.
3. Высокоорганизованный характер и тесная связь с организованной преступностью, так как наибольшее количество преступлений совершается именно организованными преступными группами.
4. Профессионализм лиц, совершающих данные преступления; преступный доход является единственным источником средств к существованию.
5. Трансграничность: существует вне государственных границ[1].

Дать характеристику преступлениям, совершаемым в сфере игорного бизнеса, можно через следующие его признаки: Чрезвычайно высокая доходность этого вида коммерческой деятельности.

- Эксплуатация человеческой слабости как источника существования игорного бизнеса (выше говорилось об азарте). Это в конечном итоге может привести к развитию игровой зависимости.
- В целом противоречивое отношение к игорному бизнесу. Во многом это вызывается противоположными стремлениями получить высокую прибыль в виде налоговых отчислений, при этом не допустить развращения общества[2].

В настоящее время предусмотрена уголовная ответственность за незаконную организацию и проведение самих азартных игр (ст. 171.2 УК РФ). Однако отмечается, что наиболее распространенным видом преступления в данной сфере является мошенничество.

Изначально такие преступления совершались самим казино для создания проигрышных ситуаций и обогащения банка заведения[3]. Однако мошенниками являются и сами игроки, использующие различные электронные средства, позволяющие увеличить выигрыш.

---

[1] См.: Киберпреступность: криминологический, уголовно-правовой, уголовно-процессуальный и криминалистический анализ: монография / науч. ред. И. Г. Смирнова; отв. ред. О. А. Егерева , Е. М. Якимова. М.: Юрлитинформ, 2016. С. 71.

[2] См.: Лихолетов А. А. Преступления в сфере игорного бизнеса: уголовно-правовые и криминологические аспекты: монография. Волгоград: ВА МВД России, 2015. С. 33.

[3] См.: Изюмова Е. С. Правовое регулирование контрольной и надзорной деятельности органов государственного управления в сфере игорного бизнеса: дис. ... канд. юрид. наук. Челябинск, 2015. С. 80–81.

Именно в этом контексте следует говорить об опасности онлайн-казино. Компьютерная безопасность – серьезный вопрос в процессе организации деятельность онлайн-казино. Заведению становятся известны персональные данные игрока, реквизиты банковских карт. Также возникает вопрос о честности как игроков, так и казино. При игре посредством компьютерных сетей доказать факт мошенничества практически невозможно.

Популярность онлайн-казино растет с каждым годом, во многом это связано с рекламой в социальных сетях.

Стоит рассмотреть одну из самых известных компаний интернет-казино – PokerStars (деятельность подобных компаний запрещена). Конечно же, компания, чей доход за 2019 год превысил 1,2 млрд долларов, из которых только один покер обеспечил 411,6 млн[1], не могла отказаться от российского рынка, который сама же считает крайне перспективным. Поэтому компания создала отдельного клиента (программный компонент системы, посылающий запросы серверу) под названием – «ПокерСтарс Сочи». Интересный «обход» российского запрета заключается в том, что в сочинском клиенте нет казино, есть лишь доступ на живую серию, проводимую в Сочи, где, в свою очередь, действует легальная игорная зона. В то время как «ПокерСтарс» дает доступ к международному онлайн-казино.

Нас же интересует рекламная кампания, которая транслировалась на российском сегменте видеохостинга YouTube. Амбассадором в России стал спортивный комментатор Дмитрий Губерниев. В одном из своих интервью он указывал на то, что покер – это тоже спорт, где требуются определенные навыки и стратегический подход[2]. Покер действительно интересный спорт, требующий математического склада ума, особых психологических умений (как и шахматы). Однако он остается азартной игрой. Опасность он представляет не для всех, а для людей с азартным характером. А учитывая доступность онлайн-казино, можно представить, насколько быстро начнет развиваться этот рынок.

На взгляд автора работы, ключевой мерой предупреждения здесь следует считать социально-психологическое воздействие на людей. Необходимо освещать негативное воздействие азартных игр на личность

---

[1] См.: Владелец онлайн-покера без лицензии купит рекламу на российском ТВ // РБК. URL: https://www.rbc.ru/technology_and_media/29/08/2019/5d66bf279a79476e6f8cfbd3 (дата обращения: 12.01.2021).

[2] Губерниев Д. Покер – это спорт! // YouTube. URL: https://youtu.be/A-_v928KV80 (дата обращения: 12.01.2021).

и экономическое состояние общества. Примерами таких мер могут являться социальные передачи, выпуск брошюр о возможности получения специальной помощи больным игроманией, проведение профилактических бесед в учебных заведениях.

Главная проблема киберпреступности – ее неуязвимость. Современные технологии (облачные данные, зеркала запрещенных сайтов) дают преступникам карт-бланш на любое преступление в Сети и уверенность в анонимности.

Поэтому единственный путь борьбы с киберпреступлениями – не дать потенциальной жертве себя обмануть.

Следует запомнить простую истину: в казино выигрывает только казино.

Список литературы

1. Агапов П. В. Противодействие киберпреступности в аспекте обеспечения национальной безопасности: монография / Акад. Ген. Прокуратуры Рос. Федерации. М., 2014.
2. Губерниев Д. Покер – это спорт! // YouTube. URL: https://youtu.be/A-_v928KV80 (дата обращения: 12.01.2021).
3. Дремлюга Р. И. Интернет-преступность. Владивосток, 2008.
4. Изюмова Е. С. Правовое регулирование контрольной и надзорной деятельности органов государственного управления в сфере игорного бизнеса: дис. ... канд. юрид. наук: 12.00.14. Челябинск, 2015.
5. Киберпреступность: криминологический, уголовно-правовой, уголовно-процессуальный и криминалистический анализ: монография / науч. ред. И. Г. Смирнова; отв. ред. О. А. Егерева , Е. М. Якимова. М.: Юрлитинформ, 2016.
6. Лихолетов А. А. Преступления в сфере игорного бизнеса: уголовно-правовые и криминологические аспекты: монография. Волгоград: ВА МВД России, 2015.
7. Севостьянов Р. А., Просвирин Е. В. Проблемы уголовно-правового регулирования организации и ведения незаконного игорного бизнеса: монография. М.: Юрлитинформ, 2013.
8. Тропинина Т. Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы: дис. … канд. юрид. наук: 12.00.08. Владивосток, 2005.

Ю. С. Гокунь

ЮРИДИЧЕСКИЕ ЛИЦА КАК ИНТЕРНЕТ-ЖЕРТВЫ: ВИКТИМОЛОГИЧЕСКИЙ АСПЕКТ

Аннотация: Тезисы посвящены изучению вопросов юридических лиц как жертв интернет-преступлений. Сделан вывод о том, что виктимность юридического лица в механизме совершения преступления в сети Интернет вызвана наличием у него право- и дееспособности, обладанием имуществом, отсутствием либо недостаточной разработкой его нормативно-правового обеспечения, отсутствием квалифицированных кадров, отвечающих за информационную безопасность, слабым обеспечением информационной безопасности, нарушениями в работе программного обеспечения и технических средств. Предложены меры по совершенствованию виктимологической профилактики юридических лиц.

Ключевые слова: юридическое лицо, жертва преступления, виктимность, преступления в сети Интернет.

LEGAL ENTITIES AS INTERNET VICTIMS: THE VICTIMOLOGICAL ASPECT

Abstract: Theses are devoted to the study of the victimological aspect of legal entities as victims of Internet crimes. It was concluded that the victimization of a legal entity in the mechanism of committing a crime on the Internet is caused by its legal and legal capacity, possession of property, the absence or insufficient development of its regulatory and legal support, the lack of qualified personnel responsible for information security, and poor security. information security, violations in the operation of software and technical means that make a legal entity vulnerable to offenders.

Key words: legal entity, crime victim, victimization.

В настоящее время Интернет оценивается как положительное явление ввиду возможности предоставления информации в кратчайшие сроки, совершения операций с деньгами, покупки и продажи недвижимости и т. д. Участниками данных отношений помимо физических лиц в подавляющем числе случаев являются юридические лица. Актуальность данной темы обусловлена необходимостью пересмотра традиционных взглядов относительно понятия жертвы преступления, а также вопросам виктимологии юридических лиц.

На сегодняшний день проблемами виктимологии преступности в Интернете и, в частности, изучением виктимологического аспекта юридических лиц как интернет-жертв занимались такие ученые, как Воронова О. С., Ильин И. В., Кабанов П. А., Скурихина А. А., Ронжина О. С., Ридван Д. В., Шевцов В. Г., Шиканов В. И. и др. Однако среди ученых и практиков продолжается дискуссия относительно вышеуказанных

вопросов, что свидетельствует о целесообразности дальнейшего всестороннего исследования данной тематики.

Объектом виктимологии является жертва, то есть физическое лицо, пострадавшее в результате совершения преступления. Считаем, что данная трактовка является ограничительной, так как полностью исключает возможность признания юридического лица жертвой преступления не только в сети Интернет, но и в целом.

Вместе с тем на возможность признания юридического лица жертвой преступления указывает такой его признак, как наличие обособленного имущества[1], на которое может посягнуть преступник: предметы мебели, компьютерная или иная техника, уставной капитал юридического лица, денежные средства, акции или все иное, имеющее какую-либо ценность.

Полагаем, юридическое лицо может являться жертвой преступления ввиду обладания им право- и дееспособности, выражающихся в его способности быть носителем прав и обязанностей, распоряжаться этими правами и иметь корреспондирующие обязанности. Наличие собственного имущества и обладание правовым статусом обязывают юридическое лицо нести ответственность за результаты осуществляемой им хозяйственной деятельности и подлежат административной ответственности за совершенные правонарушения. В гражданском праве юридические лица несут ответственность, вытекающую из нарушения обязательств. Уголовную ответственность юридические лица не несут, так как они не являются субъектами преступления[2], однако могут выступать в качестве непосредственного объекта преступных посягательств[3]. Юридические лица, реализуя свои права и обязанности, привлекают внимание правонарушителей. Последние, осуществляя мониторинг деятельности юридических лиц и используя Интернет, взламывают базы данных, похищают конфиденциальную информацию с секретами производства, провоцируют ее утечку с целью дальнейшей продажи на коммерческом рынке.

---

[1] См.: Галимова А. Ф. Право собственности юридических лиц и проблемы регулирования // Наука, образование и инновации: сборник статей Международной научно-практической конференции. В 4 ч. Ч. 3. 2016. С. 171–173.

[2] См.: Минин Р. В. Проблема формирования концепции уголовной ответственности юридических лиц в России // Юридическая наука и правоохранительная практика. 2019. № 1 (47). С. 62–68.

[3] См.: Фаткулин С. Т. Юридические лица как объект криминальной виктимологии // Виктимология. 2018. № 2 (16). С. 61–66.

Стремительное развитие сферы компьютерных технологий, увеличение количества юридических лиц, рост их значимости, наличие разнообразных организационно-правовых форм хозяйствующего субъекта, существование международных юридических лиц и некоторые другие факторы выступают в качестве аргументов, подтверждающих возможность для юридического лица стать жертвой интернет-преступления.

По мнению ряда ученых, в том числе Д. В. Ривмана, юридическое лицо не может быть жертвой преступления по причине отсутствия у него «живой души», то есть качеств, свойственных людям[1]. Однако следует отметить, что юридическому лицу так же могут быть причинены материальные убытки и нанесен ущерб его деловой репутации. Зачастую с банковских счетов организаций вследствие хакерских атак снимают крупные суммы денег. Возможны и другие способы осуществления посягательств.

В США были зафиксированы тысячи случаев кибератак, осуществленных с использованием троянской программы-вымогателя CryptoLocker. Распространение вредоносной программы происходило сразу в нескольких формах: посредством зараженных вложений, отправленных на электронную почту, через зараженные сайты и с использованием установленного в компьютер пользователя ботнета, то есть компьютерной сети, которая включает в себя несколько хостов с запущенным автономным программным обеспечением. Троян, при попадании на компьютер, зашифровывал определенные типы файлов, которые хранились на сетевых дисках. Шифрование осуществлялось с использованием криптосистемы с открытым ключом RSA. Закрытый ключ хранился на серверах, осуществляющих управление CryptoLocker. На экране компьютера отображалось предложение о расшифровке хранящихся на устройстве сведений, если платеж будет произведен в указанный срок. В противном случае произойдет удаление закрытого ключа. При несоблюдении срока, предназначенного для осуществления платежа, CryptoLocker предлагал расшифровать данные через онлайн-сервис хакеров за более высокую плату. Гарантия того, что оплата позволит расшифровать контент, отсутствовала.

Еще одним примером, получившим мировую известность, стала кибератака с использованием сетевого червя программы-вымогателя Petya, жертвами которой стали юридические лица по всему миру.

[1] См.: Ривман Д. В. Криминальная виктимология. СПб.: Питер, 2002. С. 53–66.

В Российской Федерации от хакерской атаки пострадали Роснефть, Башнефть, Сбербанк и Евраз.

В поддержку мнения о том, что юридическое лицо может быть жертвой интернет-преступления, следует упомянуть о существовании п. 1 ст. 42 УПК РФ, указывающего на то, что юридическое лицо может быть признано потерпевшим.

Юридическим лицам, как жертвам интернет-преступлений, свойственна виктимность, которая может быть выражена в том, что предприятие не уделило достаточного внимания защите данных. Как известно, технологические, производственные и коммерческие данные субъектов хозяйствования обладают высокой стоимостью. В случае их потери или утечки юридическое лицо понесет серьезный материальный ущерб, а в некоторых случаях возможна даже ликвидация юридического лица. Недостаточный уровень правового обеспечения защиты информации с начала существования юридического лица делает его легко восприимчивым к потере или утечке информации. Надлежаще оформленная нормативно-правовая база снижает уровень виктимности юридического лица, так как она выполняет две наиболее важные, с точки зрения уголовного права, функции: устанавливает правила обеспечения информационной безопасности и предусматривает ответственность сотрудников за их нарушение. Уровень виктимности юридического лица повышает и отсутствие перечня данных, подлежащих защите. Здесь потенциально важной является закрытая информация, то есть информация, доступ к которой имеет ограниченный круг лиц.

На вероятность юридического лица стать интернет-жертвой влияет отсутствие персонала, отвечающего непосредственно за защиту информации. Такую группу должны составлять специалисты в области интернет-технологий и информационной безопасности, а не сотрудники, выполняющие другие функции и частично разбирающиеся в защите данных. В ряде случаев кадровый состав штата юридических лиц не предусматривает наличие профессиональных сотрудников в IT-сфере, обеспечивающих защиту производственных, технических, коммерческих и иных данных. Все это делает уязвимым информационную безопасность юридических лиц.

Определенный прогресс в данном вопросе можно наблюдать на примере крупных компаний и фирм, в штате которых имеются специально подготовленные кадры, следящие за их информационной безопасностью. Тем не менее даже защищенные на первый взгляд юридические лица не всегда осуществляют всестороннюю защиту данных, что делает

их жертвами интернет-преступлений. Это происходит в силу всевозможных потенциальных угроз. Первой из них можно считать следующие действия сотрудников: совершение ошибок в процессе осуществления защиты данных, связанных с неопытностью, спешкой, отсутствием профессионализма, халатностью, небрежным отношением к своей работе, невнимательностью и тому подобными факторами, либо заранее спланированное совершение действий, повлекших за собой нарушение, потерю и утечку данных.

Форс-мажорные обстоятельства как аспект, связанный с виктимностью интернет-жертвы, предусмотреть практически невозможно. Особенно сложно определить конкретное обстоятельство, которое может повлиять на деятельность юридического лица. Даже крупные компании, организации, предприятия не всегда предусматривают такие чрезвычайные обстоятельства, как стихийные бедствия, пожары и т. д., способные сделать систему или базу данных беззащитной, чем могут воспользоваться преступники. В связи с чем возникает необходимость в разработке и применении специальных индивидуальных для каждого форс-мажорного обстоятельства средств защиты.

Сбои в системе, нарушение, отказ работы программного обеспечения и технических средств становятся еще одним критерием виктимности юридического лица как интернет-жертвы. Данные негативные явления возникают без вмешательства кого-либо – сами по себе из-за технических неполадок с оборудованием, а также могут быть следствием использования вируса. Последний случай предполагает наличие субъекта, внедрившего компьютерный вирус и деактивировавшего систему защиты данных. Следовательно, для недопущения вышеназванных ситуаций юридическим лицам необходимо активнее использовать программные и технические средства защиты.

Таким образом, приходим к выводу о том, что юридическое лицо в силу присущих ему особых качеств способно быть жертвой интернет-преступления. Виктимность юридического лица в механизме совершения преступления в сети Интернет вызвана наличием у него право- и дееспособности, обладанием имуществом, отсутствием либо недостаточной разработкой его нормативно-правового обеспечения, отсутствием квалифицированных кадров, отвечающих за информационную безопасность, слабым обеспечением информационной безопасности, нарушениями в работе программного обеспечения и технических средств, делающих юридическое лицо уязвимым перед правонарушителями.

Список литературы

1. Галимова А. Ф. Право собственности юридических лиц и проблемы регулирования // Наука, образование и инновации: сборник статей Международной научно-практической конференции. В 4 ч. Ч. 3. 2016. С. 171–173.
2. Минин Р. В. Проблема формирования концепции уголовной ответственности юридических лиц в России // Юридическая наука и правоохранительная практика. 2019. № 1 (47). С. 62–68.
3. Ривман Д. В. Криминальная виктимология. СПб.: Питер, 2002. 304 с.
4. Фаткулин С. Т. Юридические лица как объект криминальной виктимологии // Виктимология. 2018. № 2 (16). С. 61–66.

А. В. Двуличанский

КИБЕРТЕРРОРИЗМ: НОВЫЕ ВЫЗОВЫ И УГРОЗЫ

Аннотация: В данной статье раскрываются особенности использования информационного пространства и технических инструментов с целью осуществления террористической деятельности, предлагаются меры для предупреждения распространения террористической идеологии в информационной среде.

Ключевые слова: информационный терроризм, террористическая пропаганда, информационные вбросы, киберпространство.

CYBERTERRORISM: NEW CHALLENGES AND THREATS

Abstract: This article reveals the peculiarities of using the information space and technical tools for the purpose of carrying out terrorist activities, proposes measures to prevent the spread of terrorist ideology in the information environment.

Keywords: information terrorism, terrorist propaganda, information stuffing, cyberspace.

За последние годы значительно выросла роль использования информационных технологий в жизни личности и общества. Сегодня невозможно представить сферу жизнедеятельности, которую не коснулся бы процесс информатизации и цифровизации. В условиях глобализации одной из важных проблем, способной нанести урон целостности системе безопасности нашей страны, является бесконтрольное использование информационного пространства лицами, осуществляющими террористическую деятельность.

Основными видами информационно-технических инструментов, используемых в террористической деятельности, являются:

- интернет-ресурсы (интернет-сайты, интернет-хостинги, социальные сети, сайты знакомств, форумы);

- мессенджеры (Telegram, Viber, WhatsApp);
- средства массовой информации;
- навигационная аппаратура;
- беспилотные летательные аппараты;
- смартфоны.

С использованием мессенджеров Viber и WhatsApp была осуществлена вербовка студентки Московского государственного университета В. Карауловой, которая отправилась в Сирию для того чтобы выйти замуж за человека, с которым была знакома виртуально. При этом чаще всего вербовщик находится за пределами Российской Федерации. Данная схема вербовки показала высокую эффективность на протяжении всего периода ведения боевых действий на территории Ирака и Сирии. Кроме мессенджеров, для осуществления вербовочных подходов террористы активно используют мусульманские сайты брачных знакомств (www.nikyah.ru, www.nikah.su, www.muslima.com) и социальные сети. Основным преимуществом вербовок в Сети является возможность создания «фейковых» страниц и аккаунтов, усложняющих поиск и установление данной категории лиц силами специальных служб.

В последние годы участились случаи анонимных звонков о «минировании» административных зданий и социальных объектов с использованием IP-телефонии (через Интернет, а не через телефонные сети). Проведенными оперативно-разыскными мероприятиями российские специальные службы установили, что компьютерный след ведет на территории иностранных государств (Сирия, Украина). Анонимные звонки о минировании объектов социально-экономической сферы могут использоваться террористическими элементами в качестве способа дестабилизации общественного порядка, нанесения экономического урона, что приведет к нарушению функционирования всех ветвей власти.

Возможности, которыми в настоящее время располагает Интернет, позволяют использовать их для осуществления преступного замысла, а именно:

- террористических актов в СМИ и сети Интернет;
- передачи информации для координации деятельности участников террористического сообщества;
- вербовки новых членов в свои ряды;
- методической помощи в изготовлении самодельных взрывных устройств и проведении террористических акций;
- управления и контроля за террористическими ячейками из-за рубежа;

- использования телефонной связи для инициирования взрывных устройств;
- денежных переводов (в том числе в криптовалюте) в качестве пожертвований террористическим сообществам и организациям;
- анонимных звонков о минировании с использованием IP-телефонии.

Среди террористических интернет-ресурсов северокавказского бандподполья наиболее известны интернет-сайт «Кавказ Центр» (был зарегистрирован 14 апреля 2006 года Шведским агентством Radio och TV Verket), «ИсламДин» – официальный сайт Имарата Кавказ КБК (Объединенного Вилайята Кабарды, Балкарии и Карачая). На них размещаются пропагандистская информация, видеообращения боевиков, видеоролики с совершенными терактами и нападениями и иная информация экстремистского толка. В настоящее время доступ к большинству данных ресурсов на территории России заблокирован[1].

После совершения диверсионно-террористического акта террористические группировки активно используют информационное пространство для осуществления пропаганды с целью воздействия на общественное мнение, придания ореола мученичества (в случае если террористическую акцию совершил террорист-смертник), а также перекладывание вины и ответственности за произошедшее на силовой блок.

Замечено, что информационные вбросы, обвиняющие правоохранительные органы в совершении террористических актов, происходят после каждого резонансного террористического акта[2].

При этом наибольшая эффективность их использования достигается в период 10–12 дней после совершения резонансных террористических актов[3].

В связи с вышеизложенным целесообразно использовать меры информационной контрпропаганды с использованием возможностей

[1] См.: Борьба с терроризмом: новые вызовы и угрозы: монография / под общ. ред. В. В. Меркурьева; Университет прокуратуры Российской Федерации. М.: Проспект, 2020. С. 236.

[2] См.: Степин Д. С. Информационное воздействие террористической и экстремисткой агитации и пропаганды в сети Интернет // Криминологические проблемы регионов Крайнего Севера России / под ред. проф. А. И. Долговой. М.: Российская криминологическая ассоциация, 2015. С. 182, 184.

[3] См.: Степин Д. С. Особенности осуществления террористической агитации и пропаганды с использованием интернет-ресурсов (на примере форума «КавказЧат») // Проблемы теории и практики борьбы с экстремизмом и терроризмом: материалы научно-практической конференции. М.: Российская криминологическая ассоциация; Ставрополь: Изд-во СКФУ, 2015. С. 25–32.

средств массовой информации, блогеров, тематических групп в социальных сетях, которые должны не только опровергать информацию, размещенную террористами, но и основываясь на позитивных идеях, давать альтернативную точку зрения на произошедшее, всецело освещать вопросы, представляющие интерес для категории людей, являющихся целью террористической пропаганды.

На наш взгляд, увеличение потока информации, воспринимаемой конкретным пользователем, снижает критичность ее оценки. Использование манипулятивных технологий позволяет террористическим и экстремистским формированиям оказывать воздействие на общество.

В связи с высоким уровнем опасности террористических элементов, использующих информационно-технические средства, считаем целесообразным осуществление следующих мер по предупреждению распространения террористической идеологии:

- проведение международных конференций по контролю за киберпространством;
- осуществление контроля за использованием мировой финансовой системы с целью выявления фактов использования террористическими элементами в своих целях ее инструментов;
- введение новой статьи в Уголовный кодекс 207.1 «Заведомо ложное сообщение об акте терроризма с использованием IP-телефонии»;
- принятие международных нормативных правовых документов, разрешающих заморозку банковских активов по запросу страны – участницы соглашения, а также блокировку транзакций, использующихся для осуществления террористической деятельности без решения международных судов.

Список литературы

1. Борьба с терроризмом: новые вызовы и угрозы: монография / под общ. ред. В. В. Меркурьева; Университет прокуратуры Российской Федерации. М.: Проспект, 2020.
2. Степин Д. С. Информационное воздействие террористической и экстремисткой агитации и пропаганды в сети Интернет // Криминологические проблемы регионов Крайнего Севера России / под ред. проф. А. И. Долговой. М.: Российская криминологическая ассоциация, 2015. С. 180–184.
3. Степин Д. С. Особенности осуществления террористической агитации и пропаганды с использованием интернет-ресурсов (на примере форума «Кавказ-Чат») // Проблемы теории и практики борьбы с экстремизмом и терроризмом: материалы научно-практической конференции. М.: Российская криминологическая ассоциация; Ставрополь: Изд-во СКФУ, 2015. С. 25–32.

С. Журмухамбетова

ТЕНДЕНЦИИ РАЗВИТИЯ КИБЕРБЕЗОПАСНОСТИ В БОРЬБЕ С КИБЕРПРЕСТУПНОСТЬЮ

Аннотация: Цель работы состоит в комплексном анализе развития киберпреступности, рассмотрении предложенных существующих мер борьбы с киберпреступностью, которыми активно пользуются зарубежные страны, а также меры по устранению основных проблем в организации по борьбе с киберпреступностью.

Ключевые слова: киберпреступность, кибербезопасность, интернет-пространство.

TRENDS IN THE DEVELOPMENT OF CYBERSECURITY IN THE FIGHT AGAINST CYBERCRIME

Abstract: The purpose of the work is to provide a comprehensive analysis of the development of cybercrime, to consider the proposed existing measures to combat cybercrime, which are actively used by foreign countries, as well as measures to eliminate the main problems in the organization to combat cybercrime.

Keywords: cybercrime, cybersecurity, Internet space.

На уголовно-правовую сферу нахлынул новый вид преступлений – киберпреступность. С каждым днем уровень преступлений данного вида только повышается, а значит перед обществом и государством стоит задача повышения уровня кибербезопасности в интернет-пространстве. Для решения данной задачи необходимы правовые меры интенсивного характера, позволяющие раскрывать киберпреступления, пресекать их. В период пандемии данная проблема особо остро прочувствовалась как населением, так и государством. По данным МВД, за период 2020 года число преступлений, совершенных с использованием информационно-коммуникационных технологий, выросло на 94,6 %, тяжких и особо тяжких – на 129,7 %. Необходимо отметить, что расчетные карты использовались в преступных целях фактически в 6 раз чаще, чем в 2019 году, когда опасности наступления пандемии не существовало, а средства мобильной связи использовались в тех же целях в 2 раза чаще и более[1]. Согласно статистическим данным по киберпреступности, Брянская прокуратура за 2019 год указала, что с использованием информационно-телекоммуникационных технологий совершено 1372 преступления, что почти в 2 раза больше, чем в аналогичном периоде прошлого

[1] Краткая характеристика состояния преступности в Российской Федерации за январь–июль 2020 года». URL: https://мвд.рф/reports/item/20901417/?year=2020&month=11&day=23 (дата обращения: 10.01.2021).

года, то есть в 2018 году. Исходя из вышеперечисленного, можно сделать вывод о том, что киберпреступность в интернет-пространстве только растет, причем ее рост увеличивается в разы, что создает реальную угрозу для всей правоохранительной системы и не только[1].

В сфере кибербезопасности отсутствует эффективное взаимодействие между правоохранительными органами и прочими организациями. Ярким примером может послужить отсутствие единой системы оперативного обмена информацией с банковскими организациями, финансово-кредитными учреждениями, операторами сотовой связи. Сведения данного характера приходится получать путем бюрократии, через затяжные процедуры правового характера. Вышеперечисленное не позволяет повышать процент раскрываемости преступлений в сфере кибербезопасности, более того, усложненная процедура позволяет преступникам тщательно скрывать следы противоправных действий и уйти тем самым от ответственности. В связи с этим российский законодатель установил, что с 1 июля 2018 года оператор связи обязуется хранить в базах данных на территории Российской Федерации всю необходимую информацию с телефонов (Постановление Правительства РФ от 12 апреля 2018 года № 445 «Об утверждении Правил хранения операторами связи текстовых сообщений пользователей услугами связи, голосовой информации, изображений, звуков, видео- и иных сообщений пользователей услугами связи» (с изм. и доп.)[2]. В результате от оператора сотовой связи можно получить необходимую информацию. Данное нововведение можно считать положительным моментом в развитии кибербезопасности на территории Российской Федерации для раскрытия и расследования преступлений, однако практического применения нет, и ставится вопрос об эффективности, более того, возникает новая проблема, а именно – функционирование и хранение большого массива информации.

Еще один пробел в сфере кибербезопасности касается фишинга[3], потому что не установлена уголовная ответственность за него. В развитии кибербезопасности необходимо делать акцент на данном виде

[1] О преступлениях, совершаемых с использованием современных информационно-телекоммуникационных технологий. URL: https://genproc.gov.ru/smi/news/regionalnews/news-1731840/ (дата обращения: 10.01.2021).

[2] Собрание законодательства Российской Федерации от 23 апреля 2018 года № 17 ст. 2489.

[3] Фи́шинг (англ. phishing; от fishing – «рыбная ловля», «выуживание») – вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей: логинам и паролям.

киберпреступления, так как оно, во-первых, является наиболее привлекательным для киберпреступников по своей прибыльности, во-вторых, целью таких деяний, как правило, становятся обычные граждане, в особую группу риска попадают две категории населения: дети и пожилые люди. В-третьих, инструменты фишинга, активно совершенствуясь, приобретают более сложный характер, и распознать поддельный сайт уже непросто, так как многие из них имеют защищенное соединение (HTTPS) с подлинными сертификатами[1]. В ряде зарубежных стран фишинг и другие виды киберпреступлений строго наказываются, введена четкая дифференциация уголовной ответственности. Например, еще в начале девяностых в Нидерландах был принят Закон о компьютерных преступлениях, в котором появились новые составы киберпреступлений. А в немецком Уголовном кодексе используется специальный термин Daten, обозначающий данные, которые сохранены или передаются электронным, магнитным способами, а также компьютерные данные[2].

Если говорить непосредственно о практике применения закона, то в качестве примера можно взять США, где для реализации борьбы с киберпреступностью было создано множество спецподразделений. Например, Совместная национальная оперативная группа кибериссследований (NCIJTF), работающая с правоохранительными организациями. Их совместная работа направлена против хакеров, кибертеррористов, преступников, совершающих кражи финансовых ресурсов или персональных данных. На этом список действующих организаций по борьбе с киберпреступностью в США не ограничивается. В ФБР существует специализированное киберподразделение (Cyber Division, CyD), реализующее свою деятельность с использованием ресурсов NCIJTF. Существуют также специальные киберкоманды на всей территории США. Результатом работы этих организаций и спецподразделений являются уничтожение бот-сетей, а также создание аналитических докладов, по которым можно изучить все вопросы тенденций развития киберпреступности в сети Интернет.

Также можно отметить, что помимо правоохранительных органов в борьбе с киберпреступностью в США принимали участие

---

[1] Почему работает фишинг и как с ним бороться. URL: https://www.kaspersky.ru/blog/how-to-avoid-phishing/5411/ (дата обращения: 10.01.2021).

[2] См.: Громов Е. В. Развитие уголовного законодательства о преступлениях в сфере компьютерной информации в зарубежных странах (США, Великобритании, ФРГ, Нидерландах, Польше) // Вестник ТГПУ. 2006. Вып. 11. С. 32.

и другие органы власти. Данный положительный факт свидетельствует об активном взаимодействии и сотрудничестве органов власти друг с другом, что, возможно, будет повышать процент раскрываемости преступлений в сфере кибербезопасности. Однако и в США есть две основные проблемы: первая – это то, что США остается по-прежнему страной с наибольшим количеством зараженных ботами компьютеров в мире; и вторая – множественность жалоб от федеральных чиновников по дефициту специалистов, способных качественно проводить следствие и привлекать должным образом киберпреступников к судебной ответственности[1].

Ситуация в Российской Федерации с квалифицированными кадрами в области кибербезопасности обстоит такая же, как и в США, но более острого характера. Поэтому предлагается ввести и разработать на юридических факультетах спецкурсы по расследованию преступлений в сфере информационно-телекоммуникационных технологий, кибербезопасности и информационной безопасности. Необходимо, чтобы каждый выпускник юридического факультета обладал не только правовыми знаниями, но и должной цифровой грамотностью. Необходимо повышать цифровую грамотность населения во избежание появления новых киберпреступлений, развивать данную грамотность у сотрудников правоохранительных органов в целях пресечения киберпреступлений.

Без должной нормативной базы не может идти речь об эффективной борьбе правоохранительных органов с киберпреступностью. Не отрицается тот факт, что государство ведет активную политику по решению вышеперечисленных проблем. Однако на данный момент интенсивность разработки данного вопроса все же недостаточна.

Список литературы

1. Громов Е. В. Развитие уголовного законодательства о преступлениях в сфере компьютерной информации в зарубежных странах (США, Великобритании, ФРГ, Нидерландах, Польше) // Вестник ТГПУ. 2006. Вып. 11. С. 31–35.
2. Киберготовность США 2.0: киберпреступность и охрана правопорядка. URL: https://digital.report/kibergotovnost-ssha-2-0-kiberprestupnost-i-ohrana-pravoporyadka/ (дата обращения: 10.01.2021).
3. Краткая характеристика состояния преступности в Российской Федерации за январь–июль 2020 года. URL: https://мвд.рф/reports/item/20901417/?year=2020&month=11&day=23 (дата обращения: 10.01.2021).

[1] Киберготовность США 2.0: киберпреступность и охрана правопорядка. URL: https://digital.report/kibergotovnost-ssha-2-0-kiberprestupnost-i-ohrana-pravoporyadka/ (дата обращения: 10.01.2021).

4. О преступлениях, совершаемых с использованием современных информационно-телекоммуникационных технологий. URL: https://genproc.gov.ru/smi/news/regionalnews/news-1731840/ (дата обращения: 10.01.2021).
5. Почему работает фишинг и как с ним бороться**.** URL: https://www.kaspersky.ru/blog/how-to-avoid-phishing/5411/ (дата обращения: 10.01.2021).
6. Постановление Правительства РФ от 12 апреля 2018 года № 445 «Об утверждении Правил хранения операторами связи текстовых сообщений пользователей услугами связи, голосовой информации, изображений, звуков, видео- и иных сообщений пользователей услугами связи» (с изм. и доп.) // Собрание законодательства Российской Федерации от 23 апреля 2018 года № 17 ст. 2489.

Е. В. Киреева

КИБЕРТЕРРОРИЗМ КАК АКТУАЛЬНАЯ ПРОБЛЕМА СОВРЕМЕННОГО ОБЩЕСТВА

Аннотация: В статье рассматривается понятие кибертерроризма как разновидности киберпреступлений.

Ключевые слова: информационные технологии, киберпреступность, кибертерроризм, Интернет.

CYBER TERRORISM AS AN URGENT PROBLEM OF MODERN SOCIETY

Abstract: The article deals with the concept of cyberterrorism as a type of cybercrime.

Keywords: information technologies, cybercrime, cyberterrorism, Internet.

В основе любого общества лежит общение. Люди используют общение для получения информации и информационных продуктов. В поколении передовых технологий информация несет огромную пользу для развития личности, общества, государства, но с другой стороны, информационные технологии представляют серьезную угрозу как для отдельных индивидов, так и неопределенного круга лиц. Внедрение компьютерной техники во все сферы нашей жизни сыграло большую роль в развитии не только полезной деятельности общества, но и в развитии преступности.

Для киберпреступника компьютерные технологии – это его скрытность и увеличение дистанции от места преступления. Он может получить необходимую ему информацию на любом расстоянии путем доступа («слития информации» в сети Интернет) к практически любым секретам, как государственным, так и личным. Количество и виды

преступлений в мире информационных технологий продолжают только расти. Пока правоохранительные органы находят пути решения одних информационных преступлений, хакеры тут же придумывают новые.

Статистические данные о состоянии преступности в 2020 году свидетельствуют о том, что в целом количество зарегистрированных в стране преступлений практически соответствует уровню 2019 года, при этом наблюдается незначительный рост на 0,5 %, и в основном это связано с увеличением киберпреступлений. Число преступлений, совершенных с использованием информационно-коммуникационных технологий, выросло на 94,6 %, в том числе тяжких и особо тяжких – на 129,7 %.

Кроме того, министр внутренних дел РФ Владимир Колокольцев сообщил, что *«на общую раскрываемость негативно повлияло увеличение количества преступлений, совершенных с использованием IT-технологий, и сложности в установлении причастных к совершению таких преступлений лиц. Доля киберпреступлений повышается и достигла 23 %»*[1].

Можно предположить, что это связано с переходом в условиях пандемии большинства людей на дистанционную работу, обучение.

В настоящее время среди ученых нет однозначной позиции, какие общественно опасные деяния относятся к киберпреступлениям. Например, в Конвенции Совета Европы «О преступности в сфере компьютерной информации» указывается, что компьютерные преступления направлены «против конфиденциальности, целостности и доступности компьютерных данных и систем»[2]. В. Б. Вехов считает, что компьютерные преступления – это «общественно опасные деяния, в которых компьютерная информация является объектом преступного посягательства»[3]. С. И. Буз полагает, что «киберпреступность» представлена любым преступлением, которое может совершаться благодаря компьютерной системе или сети, в их пределах или против них[4].

[1] Интернет-портал Российской газеты // Рубрика: Происшествия. URL: https://rg.ru/ (дата обращения: 17.01.2021).

[2] Конвенция о преступности в сфере компьютерной информации (ETS № 185) [рус., англ.] (Заключена в г. Будапеште 23.11.2001) из информационного банка «Международное право» // СПС «Консультант Плюс». URL: http://www.consultant.ru (дата обращения: 12.05.2020).

[3] Картавченко В. В., Лисун Е. А. Использование высоких технологий в качестве способа совершения преступления // Проблемы и перспективы развития современной юриспруденции: сборник научных трудов по итогам Международной научно-практической конференции. Воронеж, 2015. С. 91.

[4] Буз С. И. Киберпреступления: понятие, сущность и общая характеристика // Юрист-Правоведъ. 2019. № 4 (91). С. 78.

В настоящее время наибольшую опасность приобретает такой вид компьютерных преступлений, как кибертерроризм. Это один из способов осуществления террористических действий в киберпространстве. К ним можно отнести распространение информации о различных террористических актах в Интернете. Целью кибертерроризма можно назвать стремление вывести из строя программного обеспечения какой-либо крупной компании, нарушение системы сетей электросвязи отдельной линии или целого города, получение доступа как к личной информации, так и военным секретным данным. Кроме того, это деяние может быть выражено в политически мотивированной атаке на государственную информацию, которая строго охраняется. Целями таких действий могут являться как простое запугивание населения или нарушение общественной безопасности, так и развязывание политического или военного конфликта.

И тем не менее главная цель виртуального терроризма – это получение какого-либо преимущества в решении политических вопросов, «сливание» информации, которая имеет особенную ценность для государства той или иной страны. Для осуществления своих планов преступники применяют специальное программное обеспечение, которое используется для взлома компьютерных систем тех или иных организаций.

Конечно, кибертеррористы не закладывают никаких бомб и не берут в заложники людей. Они угрожают лишь нашей виртуальной жизни коммуникационными средствами. Для этого они используют различные методы:

- Неправомерный доступ к секретным архивам, реквизитам банковских счетов и платежных систем, личным данным.
- Оказание воздействия на объекты инфраструктуры, вывод из строя отдельных компонентов, вплоть до полной остановки систем жизнеобеспечения.
- Похищение или уничтожение информации, программных средств или технических ресурсов при помощи вредоносного программного обеспечения.
- Ложные угрозы совершения атак, которые могут повлечь за собой дестабилизацию экономической или социально-политической обстановки[1].

Виртуальный террор – это относительно новое оружие для террористов и, к сожалению, очень прогрессивное. В данном случае бывает очень трудно установить личность преступника, к тому же оно

[1] См.: Космач Б. Кибертерроризм – угроза 21 века. URL: http://mirnarodov.ru/tag/kiberterrorizm (дата обращения: 17.01.2021).

может совершаться из любой точки мира, где доступно подключение к Интернету.

Суть тактики кибертерроризма в том, чтобы это преступление стало широко известно населению, шокировало общество и создавало атмосферу угрозы совершения террористического акта в любом месте.

Например, Аабид Хан занимался противоправной деятельностью, направленной на вербовку террористов через Интернет. К тому же Аабид Хан создал электронную экстремистскую энциклопедию и призывал к войне с не- мусульманами. Он вовлек в экстремистскую ячейку Хаммаада Муниш, который на момент ареста не достиг и 16-летнего возраста. На компьютере Муниш были обнаружены пропагандистские ролики «Аль-Каиды», записи с призывами к «убийствам и разрушению», а также инструкции по изготовлению напалма, взрывчатки, детонаторов и гранат[1].

В настоящее время остается актуальным вопрос, как следует квалифицировать подобного рода деяние. Ни в Уголовном кодексе Российской Федерации, ни в Федеральном законе «О противодействии терроризму» не дается определение «кибертерроризм». По своей сути кибертерроризм – это преступление, совершаемое в информационной сфере, и тогда данное деяние должно квалифицироваться по статьям, находящимся в главе 28 УК РФ. С другой стороны, кибертерроризм можно рассматривать как разновидность классического терроризма[2], и в таком случае квалификация должна происходить по соответствующим статьям главы 24 УК РФ.

Конечно, проблема противодействия кибертерроризму с каждым годом становится наиболее актуальной, и пока мы все пользуемся инновациями, за нашей информацией постоянно идет настоящая охота, хакеры придумывают все более сложные вирусы, и те, кто пытаются нас защитить, наращивают все более сложную систему защиты. Например, всем известная «Лаборатория Касперского», где сотрудники днями и ночами борются за нашу безопасность в виртуальном мире. И если они пытаются решить эту проблему изнутри, то внешне государство тоже не бездействует. В целях борьбы с данным явлением была принята Доктрина информационной безопасности Российской Федерации, утвержденная Указом Президента Российской Федерации от 5 декабря 2016 года №

[1] См.: Исламист получил 12 лет тюрьмы за кибертерроризм. URL: https://www.securitylab.ru/news/358221.php (дата обращения: 17.01.2021).

[2] Терроризм – идеология насилия и практика воздействия на принятие решения органами государственной власти, органами местного самоуправления или международными организациями, связанные с устрашением населения и (или) иными формами противоправных насильственных действий (Федеральный закон «О противодействии терроризму» от 06.03.2006 № 35-ФЗ // ст. 3).

646[1]. В Доктрине дается определение термину «информационная безопасность Российской Федерации» – состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства.

Таким образом, в XXI веке киберугрозы являются одними из наиболее опасных посягательств на общественную безопасность. Как только на смену обычному оружию приходят информационные технологии, то сразу меняется и представление о безопасности граждан. Информация в руках определенных людей становится настоящим «ядерным оружием», которое при злом умысле может нанести непоправимый ущерб. Полагаем, что правоохранительные органы в ближайшее время усовершенствуют формы и методы борьбы с киберпреступлениями.

Список литературы

1. Буз С. И. Киберпреступления: понятие, сущность и общая характеристика // Юрист-Правоведъ. 2019. № 4 (91). С. 78–82.
2. Интернет-портал Российской газеты // Рубрика: Происшествия. URL: https://rg.ru/ (дата обращения: 17.01.2021).
3. Картавченко В. В., Лисун Е. А. Использование высоких технологий в качестве способа совершения преступления // Проблемы и перспективы развития современной юриспруденции: сборник научных трудов по итогам международной научно-практической конференции. Воронеж, 2015. С. 91.
4. Конвенция о преступности в сфере компьютерной информации (ETS № 185) [рус., англ.] (Заключена в г. Будапеште 23.11.2001) из информационного банка «Международное право» // СПС «Консультант Плюс». URL: http://www.consultant.ru (дата обращения: 12.05.2020).
5. Космач Б. Кибертерроризм – угроза 21 века. URL: http://mirnarodov.ru/tag/kiberterrorizm (дата обращения: 17.01.2021).
6. Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // СПС «Консультант Плюс». URL: http://www.consultant.ru. (дата обращения: 17.01.2021).
7. Федеральный закон от 06.03.2006 № 35-ФЗ «О противодействии терроризму» (с изм. и доп.) // Собрание законодательства Российской Федерации от 13 марта 2006 года № 11 ст. 1146.

[1] Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // СПС «Консультант Плюс». URL: http://www.consultant.ru (дата обращения: 17.01.2021).

М. А. Коваленко

КРИМИНОЛОГИЧЕСКАЯ ХАРАКТЕРИСТИКА ИНФОРМАЦИОННОГО ВОЗДЕЙСТВИЯ НА НЕСОВЕРШЕННОЛЕТНИХ В СЕТИ ИНТЕРНЕТ

Аннотация: Статья посвящена криминологической характеристике информационного воздействия на несовершеннолетних в сети Интернет. Рассмотрены способы манипулирования поведением подростков с использованием характерных особенностей их возраста. Предложены рекомендации по снижению информационных угроз в отношении несовершеннолетних.

Ключевые слова: киберпреступность, несовершеннолетние, информационное воздействие, информационная безопасность.

CRIMINOLOGICAL CHARACTERISTICS OF INFORMATION INFLUENCE ON MINORS IN THE INTERNET

Abstract: The article is devoted to the criminological characteristics of information influence on minors in the Internet. The ways of manipulating with teenagers' behavior using the special characteristics of their age are described in the article. The article gives recommendations how to reduce the cyber threats for minors.

Keywords: cybercrime, minors, information influence, information security.

Современные средства коммуникации, поисковые интернет-системы, социальные сети активно используются для проведения информационного воздействия на сознание людей. Многие государства признали появление новейшего вида войн, именуемых информационными, суть которых заключается в обладании информационным преимуществом над государством противником с целью нанесения технологического, экономического, военного и морального ущерба[1].

Технологии информационного воздействия реализуются с целью манипулирования общественным мнением, продвижения интересов одних социальных групп за счет других, управления поведением индивидов. Особенно активно усиливается информационное воздействие на молодое поколение, которое является наименее подготовленным для оказания сопротивления информационным угрозам.

К числу особенностей подросткового возраста, повышающих вероятность стать жертвой киберманипуляторов, относят следующие

[1] См.: Стопоренко К. В., Ланкин В. Г. Экология информационной среды XXI в.: тенденции и риски // Избранные доклады 63-й Университетской научно-технической конференции студентов и молодых ученых. Томск: Изд-во Томского государственного архитектурно-строительного университета. 2017. С. 719.

характеристики несовершеннолетних: «повышенная внушаемость, некритичность восприятия, склонность безусловно принимать установки и мнения, доминирующие в значимых для них группах»[1], «радикализм во взглядах и оценках, максимализм в неприятии несправедливости»[2], «потребность в самоутверждении любыми средствами; нетерпимость к порицаниям»[3].

К числу факторов, способствующих негативному информационному влиянию на несовершеннолетних, следует также отнести использование интернет-технологий для общения подавляющим большинством современных детей при отсутствии необходимых представлений об информационной безопасности. Согласно исследованию «Лаборатории Касперского» «Взрослые и дети в цифровом мире» [4], основанного на результатах соцопроса в январе 2019 года, большинство родителей уже к 3 годам разрешают детям пользоваться электронными устройствами; к 4–6 годам у 54 % детей есть планшет или смартфон, а к 11–14 годам – уже у 97 %. Около 43 % детей 7–10 лет имеют аккаунты в соцсетях, при этом дети указывают в соцсетях личную информацию, которая может быть использована злоумышленниками.

Согласно проведенному автором настоящей статьи в 2019 году анкетированию 81 школьника в возрасте 11–17 лет, большинство опрошенных (71 %) считают, что в Интернете есть что-либо плохое для человека в возрасте респондента. Среди наиболее распространенных угроз, с которыми встречаются несовершеннолетние, можно отметить: знакомства и личные встречи с людьми через Интернет (62 %); просмотр веб-сайтов, на которых обсуждаются материалы экстремистского характера (45 %); способы причинения себе вреда и боли, совершения самоубийства (28 %); просмотр сексуальных изображений онлайн (18 %).

---

[1] Столяренко А. М., Сердюк Н. В., Вахнина В. В. и др. Психологические аспекты деструктивного информационно-психологического воздействия // Психология и право. 2019 (9). № 4. С. 79.

[2] Галяшина Е. И. Концепция информационной (мировоззренческой) безопасности в интернет-медиа в аспекте речеведческих экспертиз // Вестник Университета имени О. Е. Кутафина (МГЮА). 2020. № 6. С. 36.

[3] Демидова-Петрова Е. В. Криминогенность несовершеннолетних сквозь призму криминологически значимых проявлений экстремизма // Ученые записки Казанского университета. Серия Гуманитарные науки. 2018. № 2. С. 479.

[4] См.: Взрослые и дети в цифровом мире: когда онлайн встречается с офлайн, исследование «Лаборатории Касперского». URL: https://kids.kaspersky.ru/digest/issledovanie-vzroslye-i-deti-v-tsifrovom-mire-kogda-onlajn-vstrechaetsya-s-oflajnom-pdf/ (дата обращения: 16.01.2021).

Растущая цифровизация в период пандемии коронавирусной инфекции COVID-19 также увеличила уязвимость детей перед злоупотреблениями в сети Интернет, среди которых нарушения прав детей на неприкосновенность частной жизни, массовое распространение дезинформации, оказывающее сильнейшее информационное давление, травмирующее психику детей.

Сегодня масштабы и возможности информационной среды намного превосходят способности не только детей, но и взрослых людей по ее осмысленному восприятию. Проблема информационного загрязнения приобретает жизненно важную значимость для человека и общества. Происходит непрерывный рост объемов информации, возможностей информационных технологий, методики киберманипуляторов постоянно совершенствуются, при этом поиск систем контроля за этими процессами становится все более затруднительным. В результате огромное количество преступной деятельности, связанной с информационным воздействием на несовершеннолетних, совершается с использованием киберпространства: интернет-травля (кибербуллинг); побуждение к действиям сексуального характера (груминг, сексторция), общение в сети Интернет с целью совершения сексуальных действий (педофилия); онлайн-трансляции сцен сексуального надругательства над несовершеннолетними и другого вредного контента[1]; пропаганда и поддержка экстремизма и терроризма, применения насилия на территории образовательных учреждений (движения скулшутинг, колумбайн[2]), криминальной идеологии (движение АУЕ), вербовка в террористические организации; побуждение несовершеннолетних к суицидальной деятельности с использованием Интернета[3]; склонение к занятиям, опасным для

[1] См., например, дело блогера Стаса Решетникова, подозреваемого в умышленном причинении тяжкого вреда здоровью, повлекшем смерть девушки (ч. 4 ст. 111 УК), совершенного в прямом эфире стрима 2 декабря 2020 года: Блогера Reeflay задержали по делу о смерти девушки в прямом эфире // РБК. 2020. 3 дек. URL: https://www.rbc.ru/society/03/12/2020/5fc943369a794728aff6bd67 (дата обращения: 16.01.2021).

[2] См., например, дело 18-летнего Даниила Монахова, совершившего 12 октября 2020 года массовый расстрел в поселке Большеорловском Нижегородской области и покончившего жизнь самоубийством 13 октября 2020 года. В подростковом возрасте Даниил поддерживал движение «Колумбайн», планировал совершить теракт в школе, но он был предотвращен. Нижегородский стрелок сам вынес себе приговор // Коммерсантъ. 2020. 13 окт. URL: https://www.kommersant.ru/doc/4529972 (дата обращения: 16.01.2021).

[3] См., например, дело экс-схимонаха Сергия, арестованного 29 декабря 2020 года по обвинению в склонении детей к самоубийству путем проповеди, размещенной на YouTube-канале Всеволода Могучева 5 декабря под заголовком «За веру Христа мы на смерть стоим»: Сергия взяли в мирском порядке // Коммерсантъ. 2020. 29 дек. URL: https://www.kommersant.ru/doc/4529972 (дата обращения: 16.01.2021).

жизни (проезд на крыше поезда, проникновение на крыши высоких зданий); кибersталкинг (преследование жертвы с использованием Интернета с целью запугать или проявить сексуальную агрессию, расовую либо политическую ненависть); вовлечение в наркобизнес и наркопотребление и др.

Различные методы и средства информационно-психологического воздействия посредством пропаганды, скрытого убеждения, манипуляции сознанием позволяют трансформировать ценностно-смысловые ориентиры и программировать поведение несовершеннолетних пользователей сети Интернет в соответствии с деструктивными целями. Приемами манипулирования информацией являются: изменение смысла понятий; ангажированность в освещении событий, использование «фейков» для создания эмоциональной волны, ложная аргументация через пропагандистские штампы, дискредитация, перегрузка восприятия адресата избыточным количеством сообщений с целью «переполнения» негативной информацией, придание сообщению избыточной эмоциональной окраски, переход на личности, оскорбления и угрозы, троллинг, дискредитация, компрометация, попытки раскрытия конфиденциальной информации. Современные компьютерные программы позволяют определять целевые группы в Интернете, которые являются наиболее восприимчивыми к пропагандируемой информации, и способствовать насаждению онлайн-языка ненависти с помощью роботизации социальных сетей и использования бот-программ под контролем киберманипуляторов[1]. Таким образом, использование онлайн-пространства становится все менее безопасным.

В сложившейся ситуации общество теряется в поиске эффективных средств, позволяющих установить контроль и защитить сознание молодого поколения от деградации и социальной деструкции: идут дискуссии об установлении цензуры в Интернете, формировании этики информационного сообщества (введении ответственности СМИ, развитии «цифрового иммунитета»), использовании научно-технических достижений в целях прогнозирования, совершенствовании нормативно-правовой системы, государственных сил и органов, занимающихся обеспечением безопасности детей, обнаружения и предотвращения информационных угроз, наполнении информационных сфер мощным позитивным патриотическим контентом[2].

---

[1] См.: Михайленок О. М., Малышева Г. А. Роботизация социальных сетей и ее политические последствия // Власть. 2020. № 1. С. 88.

[2] См.: Овчинский А. С., Борзунов К. К. Энергоинформационные основы и приоритетные направления в борьбе с социальной деструкцией // Вестник Московского университета МВД России. 2020. № 1. С. 143–144.

Несмотря на попытки отечественного уголовного законодателя по конструированию новых составов в сфере регулирования преступлений, совершаемых в отношении несовершеннолетних в сети Интернет, следует отметить, что изменения носят не системный характер, страдают запаздыванием и пробельностью, вместе с тем для комплексного решения проблем необходима разработка единой цифровой политики, соответствующей темпам развития информационных технологий.

Существенное расширение информационных угроз в отношении несовершеннолетних требует последовательной координации и системных мер по решению общих задач со стороны государственных органов, международных организаций, владельцев информационных ресурсов, операторов связи, гражданского общества, научных кругов, а также непосредственно детей. Необходимо последовательное внедрение информационных технологий для обеспечения контроля над криминальной информационной средой; дальнейшее нормативно-правовое совершенствование; повышение уровня знаний в киберпространстве у подростков, их родителей, а также сотрудников правоохранительных органов, занимающихся проблемами киберпреступности; проведение комплексных мер профилактического характера.

Список литературы

1. Блогера Reeflay задержали по делу о смерти девушки в прямом эфире // РБК. 2020. 3 дек. URL: https://www.rbc.ru/society/03/12/2020 /5fc943369a794728aff6bd67 (дата обращения: 16.01.2021).
2. Взрослые и дети в цифровом мире: когда онлайн встречается с офлайн исследование «Лаборатории Касперского». URL: https://kids.kaspersky.ru/digest/issledovanie-vzroslye-i-deti-v-tsifrovom-mire-kogda-onlajn-vstrechaetsya-s-oflajnom-pdf/ (дата обращения: 16.01.2021).
3. Галяшина Е. И. Концепция информационной (мировоззренческой) безопасности в интернет-медиа в аспекте речеведческих экспертиз // Вестник Университета имени О. Е. Кутафина (МГЮА). 2020. № 6. С. 33–43.
4. Демидова-Петрова Е. В. Криминогенность несовершеннолетних сквозь призму криминологически значимых проявлений экстремизма // Ученые записки Казанского университета. Серия Гуманитарные науки. 2018. № 2. С. 476–486.
5. Михайленок О. М., Малышева Г. А. Роботизация социальных сетей и ее политические последствия // Власть. 2020. № 1. С. 85–92.
6. Нижегородский стрелок сам вынес себе приговор // Коммерсантъ. 2020. 13 окт.] URL: https://www.kommersant.ru/doc/4529972 (дата обращения: 16.01.2021).
7. Овчинский А. С., Борзунов К. К. Энергоинформационные основы и приоритетные направления в борьбе с социальной деструкцией // Вестник Московского университета МВД России. 2020. № 1. С. 138–144.

8. Сергия взяли в мирском порядке // Коммерсантъ. 2020. 29 дек. [Электронный ресурс] URL: https://www.kommersant.ru/doc/4529972 (дата обращения: 16.01.2021).
9. Столяренко А. М., Сердюк Н. В., Вахнина В. В. и др. Психологические аспекты деструктивного информационно-психологического воздействия // Психология и право. 2019 (9). № 4. С. 75–89.
10. Стопоренко К. В., Ланкин В. Г. Экология информационной среды XXI в.: тенденции и риски // Избранные доклады 63-й Университетской научно-технической конференции студентов и молодых ученых. Томск: Издательство Томского государственного архитектурно-строительного университета. 2017. С. 716–720.

А. В. Михайлова

КИБЕРПРЕСТУПНОСТЬ В БАНКОВСКОЙ СФЕРЕ: ПУТИ ВЫЯВЛЕНИЯ И ПРОТИВОДЕЙСТВИЯ

Аннотация: В статье рассмотрена проблема киберпреступности в банковской сфере, отражены виды и способы мошеннических действий. Для анализа текущей ситуации использованы данные Центрального банка Российской Федерации. Раскрыты основные способы выявления и противодействия киберпреступлениям в банковской сфере.

Ключевые слова: киберпреступность, преступления в Сети, банковская сфера, информационные технологии, уголовная ответственность за киберпреступления.

CYBERCRIME IN THE BANKING SECTOR: WAYS TO IDENTIFY AND COUNTERACT IT

Abstract: The article considers the problem of cybercrime in the banking sector, reflects the types and methods of fraudulent actions. To analyze the current situation, we used data from the Central Bank of the Russian Federation. The main methods of detecting and countering cybercrime in the banking sector are revealed.

Keywords: cybercrime, online crimes, banking, information technology, criminal liability for cybercrime.

XXI век считается веком информационных технологий. Однако дать объективную оценку данному явлению достаточно трудно, поскольку присутствуют как плюсы, так и минусы. Одним из минусов является набирающая обороты киберпреступность. Она определяется как «работа одного или нескольких лиц, в данном случае с колоссальными знаниями в области Интернета и цифровых технологий, использующихся

для достижения корыстных целей»[1]. Распространение сети Интернет и ценовая доступность услуг связи вызвали экспонентный рост дистанционных возможностей – от продажи товаров до получения государственных услуг. Наиболее передовым в развитии цифровых услуг оказался банковский сектор, где ежедневно растет число электронных транзакций и появляются все новые элементы экосистемы.

Следует констатировать, что правоохранительные органы сталкиваются с необходимостью выявления все новых способов и форм совершения противоправных деяний в рассматриваемой сфере. Киберпреступления в банковской сфере можно условно разделить на два вида: «преступления, связанные с осуществлением мошеннических действий, и преступления, связанные с подделкой банковских карт и осуществлением махинаций на аппаратах самообслуживания»[2].

Первый вид киберпреступлений, фишинг – «это один из видов интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователя: паролям и логинам к учетной записи в Сети»[3]. Данный вид преступлений выражается в звонках, СМС-рассылках, поддельных сайтах, в которых мошенники представляются от имени банка и противоправным путем выманивают необходимую для них информацию. С ее помощью они без труда переводят денежные средства с банковских счетов, которые впоследствии практически невозможно вернуть владельцам.

Второй вид киберпреступлений оказывается возможным в процессе завладения потерянными, украденными или поддельными банковскими картами. На устройствах самообслуживания, с технической точки зрения, он доступен в процессе установления на банкоматы или терминалы устройств, способных считывать или скопировать информацию с банковской карты клиента и обеспечить к ней несанкционированный доступ. Вследствие этого мошенники могут без прямого контакта с жертвой завладеть любой выгодной для них суммой и не оставить следов преступления, поскольку заметить установленные для данных целей устройства практически невозможно человеку, не обладающему знаниями в данной области.

---

[1] Катиева Л. М. Компьютерные преступления в банковской сфере: профилактика, предупреждение // E-Scio. 2020. № 9 (48). С. 1.

[2] Юсупова О. А. Киберпреступность в банковской сфере: современное состояние и способы защиты // Научный электронный журнал «Меридиан». 2020. № 9 (43). С. 2.

[3] Юсупова О. А. Указ.соч. С. 3.

Для различных банковских учреждений присутствуют свои идентификаторы обнаружения киберпреступлений. В общей сложности они сводятся к следующим: «обнаружение входа в систему с нового или незарегистрированного IP-адреса, попытки использования ключей, утративших сертификацию, осуществление транзакций в нетипичное для клиента время или в особо крупных размерах, привлечение недавно созданных организаций для осуществления банковских операций»[1]. Офисы банков оборудованы системами звукозаписи и видеозаписи, а также присутствует система идентификации каждого клиента.

Однако не всегда получается вовремя предотвратить данный вид преступности. Российский Центробанк в ежегодном отчете сообщил, что хищения с использованием электронных средств платежа возрастают, объем операций, проведенных без согласия клиентов, в третьем квартале 2020 года вырос до 2,5 млрд рублей против 1,9 млрд рублей годом ранее. Зампред правления Сбербанка С. Кузнецов отмечает, что «в России ухудшается ситуация с киберпреступностью: с 2013 года число киберпреступлений в России выросло в 20 раз, и ситуацию могут изменить создание единого госоргана, следящего за кибербезопасностью, и ужесточение ответственности»[2].

В настоящее время ответственность за киберпреступления предусмотрена различными нормами Уголовного кодекса Российской Федерации (далее – УК РФ). Например, в гл. 28 УК РФ устанавливается ответственность за преступления в сфере компьютерной информации, которой нелегально завладевают преступники в процессе совершения мошеннических действий. Ст. 159.3 содержит нормы об ответственность за мошенничество с использованием платежных карт, ст. 159.6 – мошенничество в сфере компьютерной информации, ст. 187 УК РФ – изготовление или сбыт поддельных кредитных либо расчетных карт и иных платежных документов с использованием средств компьютерной техники и т. п.

Тревожной тенденцией последних лет является тот факт, что несовершеннолетние намного чаще становятся фигурантами дел о хищении денежных средств с помощью использования компьютерной техники.

---

[1] Дементьева М. А., Лихачева В. В., Козырев Т. Г. Киберпреступления в банковской сфере Российской Федерации: способы выявления и противодействия // Экономические отношения. 2019. № 2. Т. 9. С. 1010.

[2] Отчет Центробанка о киберпреступности и мошенничестве. URL: https://www.angaratech.ru/press-center/novosti/otchet-tsentrobanka-o-kiberprestupnosti-i-moshennichestve (дата обращения: 15.01.2021).

С недавнего времени уменьшилась и возрастная граница по данному роду преступлений с 16 до 14 лет. Это связано с тем, что ранее портрет преступника выглядел совершенно иным образом. В основном это были злоумышленники, обладающие специальными знаниями и способные придумать вредоносное компьютерное обеспечение для этих целей, а сейчас обучиться этому не представляет особого труда, ввиду того что подробные материалы по легкому заработку можно найти на различных сайтах в сети Интернет или купить за символическую сумму. Вследствие этого многие несовершеннолетние являются соучастниками или даже создателями преступной схемы.

Проанализировав правовое регулирование и основные тенденции в рассматриваемой сфере правоохранительной деятельности, следует обсудить меры предупреждения. Противодействие киберпреступности в банковской сфере должно осуществляться комплексно[1]. Основные меры, на наш взгляд, могут быть представлены следующим образом: усиление уголовной ответственности; признание электронных документов доказательной базой при расследовании преступлений; ввод обязательной идентификации пользователей при электронном способе совершения банковских операций; разработка исключающего риск механизма в процессе совершения анонимных платежей и переводов денежных средств; создание четкого регламента взаимодействия банка и клиента.

Возрастает роль специальных знаний для выявления киберпреступлений и дальнейшего закрепления доказательственной базы[2]. Объединенными усилиями сотрудников правоохранительных органов, социальных работников и банковских служащих представляется возможным уменьшить уровень киберпреступности. Повышение осведомленности клиентов о правилах безопасности в сети Интернет окажет существенное количество на масштабы и размеры совершаемых противоправных деяний. Ведь, к сожалению, жертвами мошеннических действий чаще всего являются люди старшего возраста, которые

[1] См.: Кобец П. Н., Краснова К. А.Уголовно-правовые меры обеспечения кибербезопасности в условиях экспонентного роста киберпреступности // Обеспечение общественной безопасности и противодействие преступности: задачи, проблемы и перспективы. Материалы Всероссийской научно-практической конференции в 2 т. Симферополь, 2017. С. 205–208.

[2] См.: Краснова К. А., Кобец П. Н. Специальные знания и основные формы их использования в современном судопроизводстве // Правовое государство и правосудие. Проблемы теории и практики. Материалы VIII Международной научно-практической конференции. М., 2014. С. 302–309.

из-за доверчивости и незнания основ работы в Сети теряют достаточно крупные сбережения.

Таким образом, киберпреступления опасны тем, что совершаются дистанционно, и за короткий срок возможна большая потеря денежных средств или важной информации, в том числе относящейся к банковской тайне. Ввиду этого необходимо выстроить многоуровневую систему кибербезопасности, которая смогла бы защитить интересы как граждан, так и государства. Ведь в настоящее время кибербезопасность признается руководством страны угрозой национальной безопасности России.

Список литературы

1. 1. Дементьева М. А., Лихачева В. В., Козырев Т. Г. Киберпреступления в банковской сфере Российской Федерации: способы выявления и противодействия // Экономические отношения. 2019. № 2. Т. 9. С. 1009–1020.
2. 2. Катиева Л. М. Компьютерные преступления в банковской сфере: профилактика, предупреждение // E-Scio. 2020. № 9 (48). С. 1–7.
3. 3. Кобец П. Н., Краснова К. А. Уголовно-правовые меры обеспечения кибербезопасности в условиях экспонентного роста киберпреступности // Обеспечение общественной безопасности и противодействие преступности: задачи, проблемы и перспективы. Материалы Всероссийской научно-практической конференции в 2 т. Симферополь, 2017. С. 205–208.
4. 4. Краснова К. А., Кобец П. Н. Специальные знания и основные формы их использования в современном судопроизводстве // Правовое государство и правосудие. Проблемы теории и практики. Материалы VIII Международной научно-практической конференции. М., 2014. С. 302–309.
5. 5. Отчет Центробанка о киберпреступности и мошенничестве. URL: https://www.angaratech.ru/press-center/novosti/otchet-tsentrobanka-o-kiberprestupnosti-i-moshennichestve (дата обращения: 15.01.2021).
6. 6. Юсупова О. А. Киберпреступность в банковской сфере: современное состояние и способы защиты // Научный электронный журнал «Меридиан». 2020. № 9 (43). С. 1–4.

М. С. Орлова

ПРЕСТУПЛЕНИЯ, СОВЕРШАЕМЫЕ ПОСРЕДСТВОМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ: ОСНОВНЫЕ КРИМИНОЛОГИЧЕСКИЕ ПОКАЗАТЕЛИ И ОСОБЕННОСТИ ПРЕДУПРЕЖДЕНИЯ

Аннотация: В работе представлены основные криминологические показатели преступлений, совершаемых в информационно-телекоммуникационной сфере. Автором предложены меры, направленные на снижение и сдерживание роста исследуемых видов преступлений.

Ключевые слова: информационно-телекоммуникационные технологии, профилактика, предупреждение, преступления.

CRIMES THROUGH INFORMATION AND TELECOMMUNICATION TECHNOLOGIES: BASIC CRIMINOLOGICAL INDICATORS AND FEATURES OF PREVENTION

Abstract: The paper presents the main criminological indicators of crimes committed in the information and telecommunications sphere. The author proposes measures aimed at reducing and curbing the growth of the investigated types of crimes.

Key words: information and telecommunication technologies, prevention, prevention, crimes.

Цифровизация экономики влияет не только на образ жизни граждан, но и преступный мир в целом. 2020 год запомнился чередой ярких событий, одним из которых стало введение дистанционного формата работы, учебной деятельности, различных развлекательных мероприятий.

«Результаты проведенных исследований свидетельствуют о том, что 78 % населения России в возрасте старше 12 лет постоянно пользуются Интернетом. 90 % – заходят в глобальную сеть каждый день. Ежемесячная аудитория выросла на 6 % за 2019 год. В период пандемии потребность в интернет-покупках стала ежедневным «ритуалом» для большей части населения. Приобретение значительной части товаров осуществляется через интернет-магазины, их число выросло в 1,5 раза, а количество совершенных покупок увеличилось более чем на 25 %»[1].

[1] Что и как покупают в Интернете жители России: аналитика и статистика за 2020 год. URL: https://cms-rating.ru/chto-i-kak-pokupayut-v-internete/ (дата обращения: 06.12.2020).

Интернет-ресурсы стали основным и чуть ли не единственным источником информации для населения. Такие изменения одновременно имели и другой эффект – они стали способствовать активизации преступного поведения отдельных лиц, использующих качественно новые способы совершения преступлений, связанных с использованием информационно-телекоммуникационных технологий.

В целом массив преступлений, совершаемых с использованием информационно-телекоммуникационных технологий, за последние 5 лет увеличился более чем в 6 раз. Только за период с 2015 по 2019 год количество преступлений, совершенных с использованием информационно- телекоммуникационных технологий, по официальным данным возросло с 43,8 тыс. до 294,4 тыс. преступлений. В январе–декабре 2020 года зарегистрировано 510,4 тыс. преступлений, совершенных с использованием информационно-телекоммуникационных технологий или на 73,4 % больше, чем за аналогичный период 2019 года. В общем числе зарегистрированных преступлений их удельный вес увеличился с 14,5 % в январе–декабре 2019 года до 25,0 %. Практически все такие преступления (98,6 %) выявляются органами внутренних дел. Больше половины таких преступлений (52,4 %) относятся к категориям тяжких и особо тяжких: 267,6 тыс. (+87,5 %); больше половины (58,8 %) совершаются с использованием сети Интернет: 300,3 тыс. (+91,3 %), почти половина (42,9 %) – средств мобильной связи: 218,7 тыс. (+88,3 %). Среди наиболее часто встречаемых видов преступлений с использованием информационно-телекоммуникационных технологий за 2019 – 2020 годы были следующие: мошенничество ст. 159 УК РФ, число преступлений данного вида за 2020 год составило 210 493 преступления. Следует заметить, что ранее данный показатель был равен 119 903 преступлений, а процент прироста только за один год составил более 75,6 %. Вторым видом преступлений по распространенности являются кражи, однако уровень их прироста составил 75,5 % относительно 2019 года (173 416 преступлений). Высокие показатели темпа прироста демонстрирует такой вид преступления как «Мошенничество с использованием платежных карт», квалифицируемый по ст. 159.3 УК РФ, количество преступлений данного вида за 2020 год составило 25 820 преступлений, что на 60,2 % больше показателя года ранее. Единственным видом преступлений, показатель темпа прироста которого относительно невысок, а удельный вес среди других видов преступления незначителен, это мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ).

Число таких преступлений с 2019 по 2020 год увеличилось с отметки 687 до761 преступлений[1].

Исходя из официальных данных, мы видим, что не смотря на усилия, которые предпринимаются государством в области борьбы с преступлениями, совершаемые посредством информационно-телекоммуникационных технологий, результаты таких мер являются не столь действенными. В связи с этим, на наш взгляд, основными мерами по предупреждению указанных видов преступлений должны стать средства массовой информации, а также сами граждане страны. Например, в ряды познавательных передач еженедельно можно включать программы, которые на примере обманутых граждан покажут способы и лазейки мошеннических комбинаций, которыми пользуются злоумышленники. Также указанный способ предупреждения относится и к рекламе на ТВ-каналах, распространяется на бумажные баннеры, расположенные на транспортных остановках. Имеет место упоминание о наиболее частых способах мошеннических действий в колонках газет, такой факт обусловлен тем, что среди жертв от мошеннических действий немало граждан пенсионного возраста, которые отдают предпочтение именно бумажным источникам информации.

Кроме того, следует проводить работу с сотрудниками банков, призывать их обращать внимание на странные действия и операции, совершаемые гражданами, а также интересоваться у лиц, вызвавших подозрение, целью операции.

Сами граждане также могут оказывать содействие в предупреждении преступлений в информационно-телекоммуникационной сфере. Например, в кругу семьи и знакомых следует обсуждать случаи, связанные с хищением денежных средств, которые произошли с рассказчиком.

Также одной из мер предупреждения может являться введение дополнительных способов засекречивания персональных данных граждан, а также многослойные способы аутентификации. Например, перед тем как перевести значительную сумму денег, целесообразно задавать вопросы, которые могут заставить гражданина усомниться в правильности выполняемых им действий.

Кроме того, если гражданин часто пользуется банковскими картами, производит по ним операции, то ему следует знать и помнить о простых правилах их использования. Не всем известно, что снять деньги

[1] Состояние преступности в России за январь–декабрь 2020 года. URL: https://мвд.рф/reports/item/19412450/ (дата обращения: 12.01.2021).

с банковской карты куда проще, чем с банковского счета, поскольку для списания денежных средств требуется очное участие в процедуре списания или перевода владельца данного счета.

Еще одной профилактической мерой по сохранению безопасности денежных средств от нежелательных потерь является система компьютерной безопасности – антивирусы, среди наиболее популярных и качественных, разработчики в сфере IT-технологий выделяют Kaspersky Total Security, Bitdefender Antivirus Free Edition.

Таким образом, при изучении официальных данных можно сделать вывод об отсутствии снижения количества преступлений, совершенных с использованием информационно-телекоммуникационных сетей. Меры по предупреждению преступлений данного вида, которые применяются на практике, не очень действенны и не влекут за собой должного результата. В связи с чем предлагается дополнить уже существующие меры предупреждения мерами, предложенными автором.

Список литературы

1. Что и как покупают в Интернете жители России: аналитика и статистика за 2020 год. URL: https://cms-rating.ru/chto-i-kak-pokupayut-v-internete/ (дата обращения: 06.12.2020).
2. Состояние преступности в России за январь–декабрь 2020 года. URL: https://мвд.рф/reports/item/19412450/ (дата обращения: 12.01.2021).

И. Г. Панфилов

КИБЕРПРЕСТУПНОСТЬ – НОВАЯ КРИМИНАЛЬНАЯ УГРОЗА

Аннотация: В данной статье предложена к рассмотрению актуальная проблема современного состояния преступлений в сфере информационной безопасности. Отражена дефиниция «киберпреступность», приведена статистика преступлений, совершенных с использованием новых компьютерных технологий за 2020 год. Перечислены самые распространенные преступные деяния в области махинаций с компьютеризированной информацией, а также способы борьбы с указанными преступлениями.

Ключевые слова: информационная безопасность, киберпреступность, информационные технологии.

CYBERCRIME IS THE NEW CRIMINAL THREAT

Abstract: This article proposes to consider the current problem of the current state of crimes in the field of information security, reflects the definition of "cybercrime", provides statistics of crimes committed using new computer technologies for 2020, lists the most common criminal acts in the field of fraud with computerized information, as well as ways to combat these crimes.

Keywords: information security, cybercrime, nformation technology.

Сегодня трудно представить человека, который не пользуется техническими устройствами. Они пришли в нашу жизнь не так давно, но уже успели стать неотъемлемой частью каждого из нас. Интернет, телефон, телевизор, компьютер. Этот список можно продолжать очень долго. И все, что будет в этом списке, очень сильно упрощает нам жизнь.

Например, сотовая связь. Нам больше не надо каждый раз ехать в Суздаль, чтобы поздравить родную тетю. Теперь достаточно просто набрать ее номер на своем мобильном телефоне.

Сейчас вся наша жизнь построена на технике. Мы стали сильно от нее зависеть, а любая зависимость зачастую ни к чему хорошему не приводит. Так произошло и с зависимостью от технических устройств. Не все люди хотят работать и подчиняться законам своего государства. Но при этом каждый хочет получать деньги. Кто-то может перебороть свое желание ничего не делать и выходит на работу. А кто-то не может найти в себе силы работать и идет на различные ухищрения, которые нередко противоречат законам государства. Именно среди таких людей есть те, кто использует технические новшества в корыстных целях. И, к сожалению, таких людей становится все больше.

Количество преступлений, совершенных с применением информационных технологий, увеличивается быстрыми темпами. За январь–март

2020 года правоохранительными органами Российской Федерации зарегистрировано 101 537 преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, что на 83,9 % больше за аналогичный период 2019 года. Какой будет итоговая за 2020 год доля таких преступлений от числа всех зарегистрированных в Росси преступных деяний еще неизвестно, но уже сейчас можно сказать о совершенно неприятной и даже пугающей тенденции, заставляющей нас с большой осторожностью относиться ко всем информационным технологиям, с которыми мы взаимодействуем.

В 2019 году в МВД подсчитали, что в общем объеме правонарушений на долю преступлений с использованием IT-технологий приходится 14,5 %. Тогда как в 2018 году аналогичный показатель составлял 8,8 %.

Судебная практика показывает, что самыми распространенными преступными деяниями в области махинаций с компьютерной информацией являются:

а) неправомерный доступ к компьютерной информации (статья 272 УК РФ);

б) создание, использование и распространение компьютерных программ, которые могут нанести вред (273 УК РФ);

в) совершение мошенничества с использованием электронных средств платежа (статья 159.3 УК РФ).

Хотелось бы обратить внимание на последнее преступление, так как за 2020 год количество его совершения выросло в 9 раз. А процент раскрываемости данных преступлений, наоборот, низкий, что составляет от 47 до 55 %. На основе анализа вышеуказанной информации стоило бы задуматься о разработке методов, предназначенных для эффективного раскрытия данного вида преступлений. Уже который год тема киберпреступности не теряет своей актуальности и заботит правоохранительные органы и государство.

Например, Президент нашего государства оценил примерный ущерб от киберпреступности на начало 2021 года, он составляет 6 трлн долларов. Такое заявление было сделано 20 ноября 2020 года на саммите АТЭС в формате видеоконференции. В. В. Путин призвал страны АТЭС улучшить уровень защиты персональной информации.

С развитием цифровой и компьютерной информации деятельность злоумышленников тоже набирает силу. Преступники шагают в ногу со временем. Проблемным является еще и то, что проявления киберпреступности наблюдаются во всех областях. Это и незаконный

оборот наркотических средств, и мошеннические действия при совершении различных операций с денежными средствами, использование обманных методов с целью обогащения и множество других преступлений [1].

Чтобы повысить эффективность раскрытия данного вида преступлений, необходимо разрешить ряд проблем в работе правоохранительных органов, а именно:

- проанализировать эффективность действий по раскрытию киберпреступлений и отказаться от методов, которые не дают желаемых результатов в расследовании преступлений [2];
- наладить работу государственных организаций и судебных учреждений, проводящих экспертизу по вышеуказанным преступлениям;
- разработать в криминалистике раздел, изучающий данный вид преступности. Ведь такое направление является новым и требует создания новых задач и методов расследования;
- организовать взаимодействие правоохранителей с различными учреждениями и общественностью[3].

1 июля 2018 года в силу вступило законодательное нововведение, оно гласит, что каждый оператор сотовой связи обязуется хранить информацию (сообщения, изображения, аудио, видеоинформацию и другое) в базе данных на территории РФ. Это новшество можно отметить с отрицательной стороны. Данные методы, конечно, потребуют к себе должного внимания, ведь положение об обязанности сохранения в базах данных информации лиц в течение 6 месяцев заставляет задуматься о том, а как организовать хранение информации в базе, если с каждым разом таковых сведений будет становиться все больше и больше. Встает вопрос о расширении баз данных [4]. Еще одним минусом можно назвать и то, что

[1] См.: Быков В., Нехорошев В., Черкасов А. Совершенствование уголовной ответственности за преступления, сопряженные с компьютерными технологиями // Уголовное право. 2020. № 3. С. 9.

[2] См.: Вехов В. Б. Компьютерные преступления: способы совершения и раскрытия / Под ред. Б. П. Смагоринского. М.: Право и закон, 2019. С. 64.

[3] См.: Гончар В. В. Отдельные вопросы совершенствования подготовки кадров, специализирующихся на расследовании преступлений, совершаемых с использованием информационных технологий: сборник статей Международной научно-практической конференции // Криминалистика в условиях развития информационного общества (59-е Ежегодные криминалистические чтения). М.: Академия управления МВД России, 2018. С. 75.

[4] См.: Долгова А. И. Преступность в России начала XXI века и реагирование на нее. М.: Рос.криминол. ассоц., 2020. С. 127.

с каждым годом лица, совершающие такого рода преступления, разрабатывают что-то новое, таким образом увеличивается количество видов данных противоправных деяний, а в Уголовном кодексе по-прежнему закреплена ответственность за данные преступления в общих чертах.

Необходимо еще и учитывать тот факт, что требуется специальная подготовка кадров, назначенных раскрывать преступления в области компьютерных технологий. Стоит составить программу ознакомления сотрудников-правоохранителей с данным видом преступности (проведение семинаров, опросов, тестирования, проверка знаний и многое другое) [1].

Подводя итог вышесказанному, можно отметить, что кибербезопасность общества и государства можно будет обеспечить на должном уровне только тогда, когда со стороны правоохранительных органов будут разрешены проблемы, тормозящие процесс раскрытия преступлений, связанных с использованием преступниками новых познаний в области компьютерных технологий для достижения своего преступного умысла. Нужно сделать так, чтобы сотрудники правоохранительных органов всегда были на шаг впереди в развитии и освоении интернет-пространства, нежели лица, совершающие киберпреступления [2].

Список литературы

1. Быков В. Нехорошев А., Черкасов В. Совершенствование уголовной ответственности за преступления, сопряженные с компьютерными технологиями // Уголовное право. 2020. № 3. С. 9–11.
2. Вехов В. Б. Компьютерные преступления: способы совершения и раскрытия / Под ред. Б. П. Смагоринского. М.: Право и закон, 2019.
3. Гончар В. В. Отдельные вопросы совершенствования подготовки кадров, специализирующихся на расследовании преступлений, совершаемых с использованием информационных технологий: сборник статей Международной научно-практической конференции // Криминалистика в условиях развития информационного общества (59-е Ежегодные криминалистические чтения). М.: Академия управления МВД России, 2018. С. 73–77.
4. Дзлиев М. Общество и насилие: от традиционного терроризма к информационному // Информационные ресурсы России. 2019. № 1–2. С. 29–33.
5. Долгова А. И. Преступность в России начала XXI века и реагирование на нее. М.: Рос.криминол. ассоц., 2020.
6. Козлов В. Е. Теория и практика борьбы с компьютерной преступностью. М.: Горячая линия – Телеком, 2018.

[1] См.: Дзлиев М. Общество и насилие: от традиционного терроризма к информационному // Информационные ресурсы России. 2019. № 1–2. С. 29.

[2] Козлов В. Е. Теория и практика борьбы с компьютерной преступностью. М.: Горячая линия – Телеком, 2018. С. 343.

В.А. Сарапкин

КИБЕРПРЕСТУПНОСТЬ – АТРИБУТ СОВРЕМЕННОЙ РЕАЛЬНОСТИ

Аннотация: **В** статье рассматриваются отдельные вопросы противодействия киберпреступности, в частности, обращено внимание на некоторые факторы, обуславливающие неуклонную тенденцию увеличения количества преступлений в сфере информационных технологий; приведены соответствующие статистические данные; кратко охарактеризовано правовое регулирование противодействия киберпреступности.

Ключевые слова: **к**иберпреступность, цифровизация, противодействие преступности, прокурор.

CYBERCRIME IS AN ATTRIBUTE OF MODERN REALITY

Abstract: The article discusses certain issues of countering cybercrime, in particular, it draws attention to some factors that determine the steady trend of increasing the number of crimes in the field of information technology, provides relevant statistical data; briefly describes the legal regulation of combating cybercrime.

Key words: cybercrime, digitalization, fighting crime, prosecutor.

Компьютерные технологии являются неотъемлемой частью жизни современного общества. В очередном отчете Digital 2020, отражающем результаты ежегодного глобального исследования, проводимого агентством We Are Social[1] и платформой Hootsuite, содержатся следующие сведения[2]:

- количество интернет-пользователей в мире в январе 2020 года составляло 4,54 млрд, а в июле 2020 уже 4,57 млрд;
- в январе 2020 года в мире насчитывалось 3,80 млрд пользователей социальных сетей, в июле – 3,96 млрд;
- более 5,19 млрд человек пользуются мобильными телефонами – прирост на 124 млн (2,4 %) за последний год.

В России количество интернет-пользователей, по данным Digital 2020, составило 118 млн (81 %), а численность аудитории социальных сетей на начало 2020 года достигла 70 млн пользователей, что составляет 48 % от всего населения страны.

Очевидно, что неограниченность просторов сети Интернет, огромное количество пользователей, среди которых много тех, кто не боится нарушать законы, возможность обеспечения анонимности (особенно при

[1] Digital 2020. URL: https://datareportal.com/reports/digital-2020-july-global-statshot (дата обращения: 05.01.2021).

[2] Hootsuite. URL: https://www.web-canape.ru/business/internet-2020-globalnaya-statistika-i-trendy/ (дата обращения: 05.01.2021).

использовании DarkNet[1]), привело к тому, что, несмотря на достаточно жесткое и межправительственное противодействие киберпреступлениям, наблюдается значительный рост данных деяний из года в год.

По данным Генеральной прокуратуры Российской Федерации[2], в 2016 году в нашей стране было зарегистрировано 65 949 преступлений в сфере информационных технологий, в 2017 году уже 90 587 преступлений (рост около 37 %), в 2018 году их количество достигло 121 247. В Генеральной прокуратуре отмечают, что в период с 2013 по 2018 годы, киберпреступность продемонстрировала десятикратный рост, также в разы возросло число мошенничеств и краж с использованием информационных ресурсов, равно как и количество преступлений, связанных с хищением, удалением, блокировкой компьютерной информации с целью мошенничества. В 2019 году было зарегистрировано почти 294 000 преступлений, в 2020 году был самый заметный скачок (94,6 %) количества информационных преступлений, связано это в первую очередь с пандемией новой коронавирусной инфекции. В то же время раскрываемость таких преступлений остается достаточно низкой – 25 %[3].

Представляется очевидным, что состояние преступности данного вида, отраженное в приведенных статистических данных, явилось одним из побудительных мотивов принятия в декабре 2020 года решения о создании в структуре МВД киберполиции, в функции которой будет входить исключительно борьба с преступлениями в сфере информационных технологий.

Противодействие киберпреступности стало приоритетным направлением деятельности всех правоохранительных органов Российской Федерации и других стран мира, соответственно, и поиск результативных методов противодействия киберпреступности осуществляется многими государствами, но нельзя не отметить, что до сих пор в национальном законодательстве большинства стран, в частности, и России, отсутствует

[1] Например, если до 2014 года сбыт наркотиков происходил «из рук в руки», то с развитием цифровых технологий наркоторговцы стали использовать исключительно электронные торговые площадки в «даркнете», принимающие оплату в криптовалюте.

[2] Портал правовой статистики Генеральной прокуратуры Российской Федерации. URL: http://crimestat.ru/ (дата обращения: 05.01.2021).

[3] Материалы Координационного совещания руководителей правоохранительных органов Российской Федерации по вопросу «О состоянии работы правоохранительных и контролирующих органов по предупреждению, выявлению, пресечению и расследованию преступлений, связанных с посягательствами на безопасность в сфере использования информационно-коммуникационных технологий, включая критическую информационную инфраструктуру Российской Федерации». URL: https://genproc.gov.ru/smi/news/genproc/news-1880616/ (дата обращения: 05.01.2021).

дефиниция «киберпреступность»[1], при этом отечественный законодатель оперирует термином «киберпреступность» примерно в 5 % нормативно-правовых актов. Примечательно, что ни в одном из ключевых международных документов также нет понятия «киберпреступление», но активно используются синонимичные понятия: «информационная преступность», «преступления в сфере компьютерной информации», «компьютерные преступления»[2] или «преступления в сфере высоких технологий»[3].

Не имея возможности в рамках данной работы проанализировать, даже привести содержащиеся в различных публикациях определения киберпреступления, отметим, что их суть фактически сводится к следующему: «Киберпреступление – это любое преступление в электронной среде (сфере), совершенное при помощи компьютерной системы или сети, или против них».

К категории «киберпреступление» может быть отнесено следующее:

- неправомерный доступ к компьютерной системе;
- перехват компьютерных данных и взлом паролей;
- незаконное вмешательство в данные или в систему;
- производство, распространение или хранение средств неправомерного использования компьютеров;
- нарушение мер конфиденциальности или мер защиты данных (фишинг);
- компьютерное мошенничество или подлог;
- компьютерные преступления, связанные с использованием персональных данных;
- распространение или контроль распространения вредоносных программ;
- действия, предполагающие использование компьютера в целях причинения личного вреда;
- действия, предполагающие использования компьютера в целях содействия террористическим актам.

[1] Приставка «кибер» (cyber) во всем мире используется для обозначения чего-то, относящегося к компьютерам, цифровым технологиям и т. п.

[2] См.: Малайзия, Закон о компьютерных преступлениях (Computer Crimes Act) 1997 года; Шри-Ланка, Закон о компьютерных преступлениях (Computer Crime Act) 2007 года; Судан, Закон о компьютерных преступлениях (Computer Crimes Act) 2007 года.

[3] См.: Индия, Закон об информационных технологиях (Information Technology Act) 2000 года; Саудовская Аравия, Закон о преступлениях в сфере ИТ (IT Criminal Act) 2007 года; Боливарианская Республика Венесуэла, Специальный закон о преступлениях в сфере информационных технологий (Ley Especial contra los Delitos Informáticos) 2001 года; Вьетнам, Закон об информационных технологиях (Law on Information Technology) 2007 года.

Сеть Интернет стремительно развивается с середины XX века, что предопределило освоение преступниками нового поля деятельности – сферы информационных технологий и массовых коммуникаций, а с начала XXI века эти процессы приобрели лавинообразный характер.

Трансграничный характер киберпреступности стал причиной выработки единого международного законодательства, позволяющего государствам скоординировано бороться с нею. В 2001 году была принята Конвенция Совета Европы о киберпреступности – один из главных международных документов, содержащий унифицированные рекомендации по реализации мер, которые необходимо принять для снижения количества преступлений и пресечение возникновения новых, а также предполагающий расширение взаимодействия между странами в борьбе с киберпреступностью. Также Конвенция предполагает расширение взаимодействия между странами в борьбе с киберпреступностью и внесение соответствующих поправок в законодательство отдельных стран, позволяющих более слаженно проводить работу по снижению активности «киберпреступников».

Помимо международных нормативно-правовых актов также существуют следующие межправительственные соглашения в сфере борьбы с киберпреступностью:

1. Соглашение о сотрудничестве в борьбе с преступлениями в сфере компьютерной информации, принятое государствами-членами Содружества Независимых Государств в 2001 году (ратифицировано в РФ в 2008 году). Цель данного соглашения заключается в более тесном правовом сотрудничестве и выработке единого законодательства для всех стран Содружества в борьбе с преступлениями в сфере информационных технологий. В этом соглашении определены основные термины, общие положения киберпреступности, а также уголовно-наказуемые деяния, названы компетентные органы государств-членов, между которыми осуществляются взаимодействия, формы сотрудничества и др.
2. Соглашение между правительствами государств – членов Шанхайской организации сотрудничества об обеспечении международной информационной безопасности. В данном документе сформулированы основные угрозы в области международной информационной безопасности, основные направления, принципы и механизмы сотрудничества.
3. Соглашение о кибербезопасности между странами Лиги Арабских Государств, вырабатывающее юридические основы для защиты населения и интересов государства от преступлений в сфере информационных технологий.

Применительно к теме исследования в качестве основных отечественных нормативных источников следует указать Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 08.06.2020) «Об информации, информационных технологиях и о защите информации» (с изм. и доп., вступ. в силу с 01.01.2021), Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» и конечно же Уголовный кодекс РФ, в котором непосредственно преступлениям в сфере компьютерной информации[1] посвящена 28 глава, содержащаяся ст. 272 «Неправомерный доступ к компьютерной информации», ст. 273 «Создание, использование и распространение вредоносных компьютерных программ», ст. 274 «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей», а также ст. 274.1 «Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации».

В заключение отметим, что ведущие мировые специалисты в IT-сфере единодушны во мнении, что в обозримом будущем сохранится тенденция к росту количества преступлений, совершаемых в сфере информационно-коммуникационных технологий, соответственно, необходимо разрабатывать новые и совершенствовать имеющиеся методы противодействия киберпреступности. Кроме того, для обеспечения эффективности такого противодействия и исследования киберпреступности в целом необходимы подготовленные специалисты. На это было обращено внимание Генеральным прокурором Российской Федерации, в частности, одной из задач совершенствования системы профилактики и раннего выявления преступлений, совершенных с использованием IT-технологий и компьютерной информации, была названа следующая: «учитывая специфику их выявления, стремительное распространение криминального использования виртуальных активов, компьютерных атак на критическую информационную инфраструктуру государства необходимо внедрять специализацию сотрудников, осуществлять их профессиональный отбор, добиваться устойчивого повышения раскрываемости преступлений»[2].

[1] Следует отметить, что понятие «компьютерная информация», содержащееся в примечании 1 к ст. 272 УК РФ, нельзя признать идеальным.

[2] Материалы Координационного совещания руководителей правоохранительных органов Российской Федерации по вопросу «О состоянии работы правоохранительных и контролирующих органов по предупреждению, выявлению, пресечению и расследованию преступлений, связанных с посягательствами на безопасность в сфере использования информационно-коммуникационных технологий, включая критическую информационную инфраструктуру Российской Федерации». URL: https://genproc.gov.ru/smi/news/genproc/news-1880616/ (дата обращения: 05.01.2021).

Список литературы

1. Материалы Координационного совещания руководителей правоохранительных органов Российской Федерации по вопросу «О состоянии работы правоохранительных и контролирующих органов по предупреждению, выявлению, пресечению и расследованию преступлений, связанных с посягательствами на безопасность в сфере использования информационно-коммуникационных технологий, включая критическую информационную инфраструктуру Российской Федерации». URL: https://genproc.gov.ru/smi/news/genproc/news-1880616/ (дата обращения: 05.01.2021).
2. Проект всестороннего исследования проблемы киберпреступности // Организация Объединенных Наций. Нью-Йорк, февраль 2013.

Ш. Саргсян

МЕЖДУНАРОДНОЕ СОТРУДНИЧЕСТВО В БОРЬБЕ С КИБЕРПРЕСТУПНОСТЬЮ: ОТДЕЛЬНЫЕ ПРОБЛЕМЫ И ПУТИ ИХ РЕШЕНИЙ

Аннотация: В работе рассмотрены отдельные проблемы международного сотрудничества в борьбе с преступлениями в цифровой сфере, а также сформулированы предложения для их решения.

Ключевые слова: киберпреступление, IT-сфера, международное сотрудничество, экстрадиция.

INTERNATIONAL COOPERATION IN THE FIGHT AGAINST CYBERCRIME: SPECIFIC PROBLEMS AND WAYS TO SOLVE THEM

Abstract: The article deal with the relevance and problems of international cooperation in criminal cases in the IT-sphere, also it suggests possible solution of them.

Keywords: international cooperation, cybercriminal, cybercrime, IT-sphere, extradition, international treaty.

В настоящее время невозможно представить жизнь современного человека без компьютерных технологий. Информационно-технологическая сфера нашей жизни за последнее десятилетие сделало огромный рывок. Но последствия данного рывка не только положительные, но и отрицательные.

Специалисты отмечают, что поступательное и активное развитие Интернета открыло широкие возможности для преступников, что

послужило причиной значительного роста преступлений в данной сфере[1]. Это же подтверждают статистические данные МВД РФ, согласно которым за период с января по ноябрь 2020 года наблюдается значительный рост преступлений с использованием IT-технологий. В частности, на 81,6 % увеличилось количество краж с использованием телекоммуникационных систем[2].

Более того, у преступников появилась возможность совершать противоправные деяния, находясь на большом расстоянии от места преступления, что, несомненно, усложняет процесс их поимки. Зачастую киберпреступники действуют на территории чужих государств, рассчитывая на то обстоятельство, что правоохранительные органы государства, на чьей территории совершено преступление, не имеют властных полномочий на территории того государства, где они находятся, и, следовательно, вероятность того, что они останутся безнаказанными, ощутимо увеличивается.

Также стоит обратить внимание на то обстоятельство, что немалая часть киберпреступлений ставит под угрозу не только конфиденциальность личной жизни и безопасность обычных граждан, но и суверенитет и безопасность самого государства. Целью таких преступных деяний является не только пропаганда идей определенной группы, но также незаконный сбор данных, незаконный доступ в информационную среду органов власти того или иного государства, что впоследствии может подвергнуть опасности жизнь и безопасность большого количества людей и воспрепятствовать полноценному функционированию органов государственной власти. Например, в январе 2009 года вирус Conficker заразил военную технику Франции, вследствие чего истребители не функционировали должным образом и не смогли взлететь[3]. В декабре 2013 года хакеры заразили вредоносным программным обеспечением компьютеры участников G20, проходившего в Санкт-Петербурге, и получили доступ к секретным данным[4].

---

[1] Решняк М. Г. Современные проблемы действия уголовного законодательства Российской Федерации и отдельных зарубежных стран, связанные с цифровизацией преступной деятельности // Безопасность бизнеса. 2020. № 6. С. 54–55.

[2] Краткая характеристика состояния преступности в Российской Федерации за январь–ноябрь 2020 года. URL: https://мвд.рф/reports/item/22501861/ (дата обращения: 27.12.2020).

[3] Истребители ВМС Франции не смогли взлететь из-за компьютерного вируса. URL: https://xakep.ru/2009/02/09/47082/ (дата обращения: 17.01.2021).

[4] 20 самых громких киберпреступлений 21 века. URL: https://zen.yandex.ru/media/ id/ 5c9b21d83bbd5d00b356a271/20-samyh-gromkih-kiberprestuplenii-21-veka-5c9b232c5e29d000b 387248b (дата обращения: 17.01.2021).

Все это подтверждает актуальность усиления борьбы с киберпреступлениями и необходимость международного сотрудничества в данной сфере с целью обеспечения безопасности и правопорядка.

Международному сотрудничеству в сфере уголовного судопроизводства посвящена отдельная глава в Уголовно-процессуальном кодексе Российской Федерации. Также источниками международного сотрудничества, помимо УПК РФ, являются международные договоры России с другими государствами и принцип взаимности.

В настоящий момент можно выделить три основные формы международного сотрудничества в сфере уголовного судопроизводства:

1. Выдача лиц для уголовного преследования или исполнения приговора (экстрадиция).
2. Исполнение запросов (поручений) о производстве следственных и иных процессуальных действий (это может быть, например, производство допросов, обысков и других действий, направленных на собирание доказательств; осуществление задержания; вручение процессуальных документов, вызовов и извещений; и др.).
3. Передача осужденных к лишению свободы лиц для отбывания наказания.

Необходимо отметить, что при осуществлении каждой из вышеназванных форм международного сотрудничества государства сталкиваются с большим количеством факторов, осложняющих, а в ряде случаев мешающих полноценному сотрудничеству. Остановимся на некоторых из наиболее распространенных коллизий, с которыми сталкиваются государства.

В частности, в сфере экстрадиции до настоящего времени не определен процессуальный статус лиц, подлежащих выдаче. По нашему мнению, сам по себе термин «выдача преступника» является некорректным, так как он в определенной степени не соотносится с презумпцией невиновности. Как известно, преступником лицо может быть названо лишь после вступления в законную силу обвинительного приговора суда. Для иностранного государства, обращающегося в Российскую Федерацию о выдаче преступника, это лицо находится в статусе обвиняемого или подозреваемого; при этом экстрадированный может оказаться невиновным в совершении того преступления, в котором его обвиняют.

В Уголовно-процессуальном кодексе РФ такой субъект как «выдаваемое лицо» не упомянут, а значит, не определены его процессуальные права и обязанности. Однако фактически данные лица участвуют

в уголовном процессе. Из этого правового пробела вытекает много проблем, например, реализация такими лицами права на защиту[1].

Не следует также забывать, что киберпреступники могут совершать противоправные деяния, находясь на территории таких государств, в которых за это деяние не предусмотрено уголовного наказания или предусмотрено более мягкое, чем в стране совершения, наказание. К подобным странам относятся Доминиканская Республика, Гаити, Гондурас, где правовая база в сфере IT-технологий и киберпреступлений не развита в должной мере, что позволяет преступникам избегать наказаний за совершенные преступления.

Несомненно, вышеназванные аспекты не являются единственными. Существует множество препятствий для осуществления международного сотрудничества в сфере уголовного судопроизводства, и основной причиной наличия коллизий является тот факт, что развитие информационных технологий значительно опережает развитие международной и национальной нормативно-правовой базы. Считаем, что в УПК РФ необходимо внести соответствующие дополнения, направленные на усовершенствование процесса международного сотрудничества, иначе есть риск возникновения ситуации, когда быстро развивающаяся IT-сфера выйдет из-под контроля, что приведет к значительному росту преступлений в информационной сфере.

В связи с этим, по нашему мнению, следует предпринять ряд действий для предупреждения вышеописанной ситуации, а именно:

1. Сформулировать и создать международный правовой акт, к примеру, Декларацию о всеобщих правилах кибербезопасности, которая будет подписана всеми государствами. На основе Декларации можно будет разработать международный договор о правилах кибербезопасности, подписантами которого станут все государства с развитыми IT-технологиями.
2. В рамках правоохранительной системы каждого государства целесообразно создать отдельный специализированный орган, который будет заниматься исключительно киберпреступлениями в сотрудничестве с организациями и учреждениями, которые занимаются обеспечением кибербезопасности. Примером такой деятельности может служить союз «Лаборатории Касперского» с Интерполом. Кроме того, постоянно проводятся тренинги для

[1] См.: Жужгина А. А. Международное сотрудничество в сфере уголовного процесса: проблемы экстрадиции киберпреступников // Молодой ученый. Международный научный журнал. 2020. № 21 (311). С. 249–323.

офицеров Интерпола с целью передачи опыта в вопросах анализа вредоносных программ, обнаружения цифровых следов и улик, а также исследования финансовых угроз[1]. Полагаю, что ориентируясь на данный опыт, можно создать международный аналог, где организации, занимающиеся кибербезопасностью, будут помогать международным органам борьбы с киберпреступностью.

3. В структуре Интерпола и Европола создать специализированный отдел, оперативно реагирующий на запросы. Данное предложение связано с тем, что преступления в цифровой среде необходимо расследовать как можно быстрее, так как цифровой след меняется и / или исчезает достаточно быстро.

Автор сознает, что вышеизложенные предложения являются дискуссионными, но считает, что они могут в определенной мере способствовать, если не сокращению количества преступлений в киберпространстве, то, по крайней мере, повышению эффективности расследования данных преступных деяний и в целом оказать влияние на повышение кибербезопасности.

Список литературы

1. Жужгина А. А. Международное сотрудничество в сфере уголовного процесса: проблемы экстрадиции киберпреступников // Молодой ученый Международный научный журнал. 2020. № 2(311). С. 249–323.
2. Несмеянов А. А. Основные проблемы борьбы с преступлениями в сфере высоких технологий // Вестник Восточно-Сибирского института МВД России. 2014. № 4 (71). С. 43–48.
3. Решняк М. Г. Современные проблемы действия уголовного законодательства Российской Федерации и отдельных зарубежных стран, связанные с цифровизацией преступной деятельности // Безопасность бизнеса. 2020. № 6. С. 54–61.

[1] Несмеянов А. А. Основные проблемы борьбы с преступлениями в сфере высоких технологий // Вестник Восточно-Сибирского института МВД России. 2014. № 4 (71). С. 43–48.

Т. С. Сидорова

К ВОПРОСУ О СОВЕРШЕНСТВОВАНИИ СИСТЕМЫ МОНИТОРИНГА ДОСТУПНЫХ ДЛЯ ПОДРОСТКОВ ИНФОРМАЦИОННО-РАЗВЛЕКАТЕЛЬНЫХ РЕСУРСОВ В ЦЕЛЯХ НЕДОПУЩЕНИЯ РАСПРОСТРАНЕНИЯ КОНТЕНТА НЕГАТИВНОГО И ДЕСТРУКТИВНОГО СОДЕРЖАНИЯ В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ ИНТЕРНЕТ

Аннотация: В статье рассмотрены наиболее актуальные вопросы, связанные с реализацией мониторинга информационно-коммуникационной сети Интернет. Даны классификация и описание основных видов опасностей, с которыми могут столкнуться подростки в информационном пространстве. На основе представленной классификации проработаны вероятные пути разрешения обозначенных проблем, а также предложены варианты по совершенствованию системы мониторинга информационно-развлекательного контента и интернет-ресурсов в целях своевременного выявления контента деструктивного содержания и недопущения негативного влияния с его стороны на психическое развитие и социализацию несовершеннолетних.

Ключевые слова: мониторинг, негативный контент, информационно- современные информационные технологии.

ON THE ISSUE OF IMPROVING THE MONITORING SYSTEM OF INFORMATION AND ENTERTAINMENT RESOURCES AVAILABLE FOR ADOLESCENTS IN ORDER TO PREVENT THE SPREAD OF NEGATIVE AND DESTRUCTIVE CONTENT ON THE INTERNET

Abstract: In the article the author considers the most pressing issues related to the implementation of monitoring of the information and communication network of the Internet; a classification and description of the main types of dangers that teenagers may face in the information space are given; on the basis of the presented classification, probable ways of resolving the identified problems have been worked out, and options have been proposed for improving the monitoring system of infotainment content and Internet resources in order to timely identify destructive content and prevent its negative impact on the mental development and socialization of minors.

Key words: monitoring, negative content, modern information technologies.

Развитие коммуникативных навыков, в том числе познаний в использовании сети Интернет, у современных подростков происходит все интенсивнее с каждым годом. Современная молодежь с ранних лет начинает осваивать технические средства с их сервисами, играми

и сайтами различного характера, которые зачастую представляют большую опасность и угрозу для начинающих пользователей.

Всемирная сеть включает в себя следующие виды опасности, которые подстерегают несовершеннолетних пользователей:

1. *Социальные сети*. Множество онлайн-платформ, которые используются для общения, знакомств, развлечения и работы, являются непосредственными деформаторами коммуникативных способностей подрастающего поколения, так как виртуальное общение, безусловно, проявляется как вседозволенность и безнаказанность Сети, что вводит в заблуждение о том, что ребенок может вести себя также и при реальном общении, а это, в свою очередь, является лишь иллюзией. Кроме того, зачастую общение с «реальными» людьми может представлять опасность вовлечения в какие-либо действия противозаконного характера, а также угрозу для жизни и здоровья от лиц, предлагающих личные встречи с целью «познакомиться поближе или прогуляться», которые могут негативно закончиться для самого несовершеннолетнего.

2. *Интернет-сайты*. Множество интернет-площадок, первоначально кажущиеся безобидными для взрослых, могут носить деструктивный контент, склоняющий подростков к суицидальному поведению. Распространение молодежных субкультур, таких как эмо, готы, хикикомори, пропагандирующих депрессивный (замкнутый) взгляд на жизнь и превозносящих суицид как способ разрешения многих жизненных проблем, включая социальную отчужденность подростка, мнимое «непонимание со стороны взрослых», желание выделиться «из общей массы», то есть «совершишь суицид – все будут плакать по тебе, будут помнить, потому что ты сейчас никто, а завтра станешь «героем дня».

3. *Игры, пропагандирующие насилие и девиантные формы поведения*. Пользующиеся популярностью среди подростков игры Bully (симулятор школьного хулигана), серия Grand Theft Auto (GTA) (пропагандирующая и допускающая изощренные сцены насилия и девиаций различных видов – пропаганда расизма, гомосексуализма, социофобии и пр.), серии игр Mafia, Yakuza, позволяющие взять на себя роль представителя криминального мира, принимать участие в различных преступлениях, в том числе и с применением радикальных методов грабежей и разбоев (расстрел из гранатометов, наезд на людей при помощи специальной техники, использование холодного оружия и спортинвентаря), иных противоправных действий (мошеннических операций, торговли наркотическими средствами и оружием, контрабанды) с целью достижения ведущих позиций в криминальной иерархии; игровой контент

по мотивам серии художественных фильмов Saw (англ. – «Пила»), где игрок вовлекается в смертельную игру, организованную главным антагонистом «Конструктором», при этом каждое испытание представляет собой изощренную пытку, сопровождающуюся неприятными сценами смертей посредством ампутации конечностей, обезглавливания, сжигания, использования кислоты и пр.

Безусловно, каждая из указанных игр имеет возрастной рейтинг и соответствующую маркировку. Однако большинство родителей попросту не обращают внимания на ознакомительные и презентационные материалы по играм перед их приобретением или скачиванием в Сети, тем самым допуская своего ребенка к материалам, наполненным шок-контентом или контентом, опасным для психики несовершеннолетнего. С введением возрастного рейтинга, установленного Федеральным законом Российской Федерации от 29 декабря 2010 года № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию», эта проблема получила возможность фактического разрешения.

Однако как быть с игровым контентом, который распространялся в свободном доступе до принятия соответствующего федерального закона, или с имеющим международную классификацию рейтинговых показателей? Этот контент представляет наибольшую опасность для современных подростков. Не все родители понимают рейтинговые отметки по типу «М», как потенциально опасные для подростков. В международной классификации «М» означает – Mature, то есть контент для взрослых лиц, достигших возраста совершеннолетия, который за рубежом наступает с 21 года. Например, аннотация к лицензионной версии игры GTA имеет подобную отметку на всех интернет-ресурсах, распространяющих его официально; однако, если мы затронем официальную онлайн-статистику на сайте компании-правообладателя Rockstar[1] или различных стриминговых и игровых платформ (например, Steam или Epic Game Store), то получим сведения, что более 70 % игроков в GTA-online представляют подростки в возрасте от 12 до 17 лет. Эта статистика репрезентативна и, безусловно, по сути обесценивает институт возрастной и контекстной маркировки контента на современном этапе.

Вторая проблема касается доступа подростков к игровому контенту, не обладающему соответствующей запретной маркировкой (то есть распространявшемуся до вступления в законную силу Федерального закона

[1] См.: Официальный сайт компании Rockstar Games. URL: https://www.rockstargames.com/ (дата обращения: 25.12.2020).

«О защите детей от информации, причиняющей вред их здоровью и развитию»).

Популярностью у многих подростков продолжают пользоваться игры серии Manhunt (англ. – «Охота на человека») и The Punisher (англ. – «Каратель»), не имевшие на релизе в России возрастных рейтингов. Игры отличаются повышенной степенью жестокости и рассчитаны на игровую симуляцию «казней врагов в игровом пространстве изощренными способами» (например, убийство пневмопистолетом, молотком, обезглавливание бензопилой, причинение телесных повреждений врагам «при допросах» при помощи различных механизмов (мясорубки, гидравлического пресса, электросверла), оружия, иных орудий и даже при помощи животных (например, нанизывание врага на рог носорога), а также прочий жестокий контент). Компьютерная игра Manhunt и ее продолжение были запрещены на российском информационном пространстве, однако в Сети до сих пор можно встретить их нелицензионные копии (прежде всего на различных torrent-ресурсах и пиратских сайтах), что, безусловно, вызывает определенные опасения.

4. *«Ненавязчивая» реклама на* сайтах разного характера может носить также негативный контент: проявление молодежного экстремизма, расовая, национальная или религиозная вражда, рецепты и изготовление средств, оказывающих психотропное воздействие на организм человека, порнографические материалы – все это ведет к необратимым последствиям в развитии еще не сформировавшейся психики подростков.

Безусловно, обозначенные проблемы требуют надлежащей правовой оценки и проработки дополнительных путей по совершенствованию методики контроля интернет-среды и предупреждению противоправного влияния в киберпространстве.

Остановимся отдельно на некоторых из них.

Во-первых, разрешение обозначенных проблем видится в совершенствовании системы мониторинга, а именно в развитии программ с функцией родительского контроля, которые блокируют доступ ребенка к опасной информации деструктивного характера.

При этом важным фактором является непосредственный контроль за поведением ребенка, его высказываний и настроения, что, безусловно, возлагает большую ответственность на всех субъектов профилактики, включая родителей и родственников, в связи с наблюдением за несовершеннолетним.

Кроме того, должное внимание следует уделить и контенту, который просматривает подросток, независимо от моды на него или его

популярности (например, сеть TikTok и пр.), чтобы вовремя предпринять необходимые меры.

Во-вторых, необходимо проработать четкую систему индикаторов, позволяющих определять деструктивный для психического здоровья подростков контент и своевременно пресекать его распространение в сети Интернет. Одним из подобных решений видится запрет на свободную передачу вспомогательного программного обеспечения (по типу VPN или Tor), позволяющего обходить запреты, установленные Роспотребнадзором на нежелательный контент.

В-третьих, пересмотреть устаревший информационно-цифровой контент на предмет его соответствия новым требованиям и позициям в определении его нежелательности или деструктивности для психики подростка.

Другим немаловажным аспектом в мониторинге выступает правовая и техническая грамотность родителей. В век развития современных информационных технологий и цифровизации общественных отношений родители, обладающие познаниями в области молодежной культуры, способны первыми обнаруживать деструктивный и шокирующий контент и своевременно ограждать своих детей от его распространения или ознакомления с ним.

Проведение онлайн-курсов компьютерной и культурологической грамотности среди родителей, например, со стороны общественных объединений, органов государственной власти и образовательных учреждений, позволит устранить пробелы между поколениями, помочь родителям понять своих детей лучше и своевременно реагировать на любые проявления негативного характера.

Предложенные пути по совершенствованию мониторинга не являются исчерпывающими, однако их применение в условиях современных реалий позволит обезопасить подрастающее поколение от негативной информации, уберечь подростков от необдуманного и суицидально-депрессивного поведения и обеспечить молодежи достойное будущее.

Список литературы

1. Попова Е. А. Предупреждение негативного информационного воздействия в сети Интернет. URL: https://xn--90aeohcucbsffh.78.xn--b1aew.xn--p1ai/document/12254596 (дата обращения: 25.12.2020).

В. В. Сынков

КИБЕРПРЕСТУПНОСТЬ – ВЫЗОВ XXI ВЕКА

Аннотация: Статья посвящена рассмотрению киберпреступности, как нового и весьма опасного явления XXI века. Проводится некоторый статистический анализ состояния киберпреступности в России, а также освещается зарубежная практика.

Ключевые слова: киберпреступность, виртуализация, компьютеризация, общество постмодерна.

CYBERCRIME – THE CHALLENGE OF THE 21ST CENTURY

Abstract: The article is devoted to the consideration of cybercrime as a new and very dangerous phenomenon of the 21st century. Some statistical analysis of the state of cybercrime in Russia is carried out, as well as foreign practice is highlighted.

Keywords: cybercrime, virtualization, computerization, postmodern society.

Одним из неотъемлемых свойств общества постмодерна является «виртуализация» жизнедеятельности, вызванная современным техническим прогрессом. Как отмечают Andrew Goldsmith и David S. Wall, за 25 лет существования Интернета[1] он привлек более половины жителей планеты – по состоянию на 30 июня 2019 года количество пользователей Интернета составило около 4,5 млрд человек[2]. Отметим, что в 2020 году количество пользователей сети Интернет только увеличилось, причем, довольно значительно – по состоянию на 30 сентября 2020 года их количество составило 4 929 926 187 человек[3].

Уход человека в виртуальную реальность закономерно привел к виртуализации преступности. Это вызвало появление такого феномена, как киберпреступность. Некоторые ученые определяют киберпреступность через средство или орудие, в качестве которых выступает вредоносная компьютерная программа или программно-техническое

[1] Заметим, что Интернет существует гораздо большее количество лет. Историю его следует вести с 1969 года (см.: Интернет // Википедия: свободная энциклопедия. 2020. URL: https://ru.wikipedia.org/wiki/Интернет (дата обращения: 29.12.2020). Таким образом, к 2020 году «возраст» Интернета составляет 51 год.

[2] Goldsmith A., Wall D. S. The seduction of cybercrime: Adolescence and the thrills of digital transgression // European Journal of Criminology. URL: https://journals.sagepub.com/doi/full/10.1177/1477370819887305 (дата обращения: 29.12.2020). Здесь и далее перевод авторский.

[3] Internet usage statistics. The Internet Big Picture. World Internet Users and 2020 Population Stats // Internet World Stats: Usage and Population Statistics. 2020. URL: https://www.internetworldstats.com/stats.htm (дата обращения: 29.12.2020).

средство, подключенное к компьютерной сети или сотовому оператору связи[1]. Такое определение представляется нам спорным по следующим причинам. Во-первых, средство вовсе не выступает в данном случае определяющим звеном. Marleen Weulen Kranenbarg, Stijn Ruiter и Jean-Louis Van Gelder отмечают, что большинство криминологических исследований посвящаются cyber-assisted deviant behaviour, то есть преступлениям, совершаемым с помощью компьютерных технологий (выделено мной – В. С.). А вот cyber-dependent offendings не учитываются[2]. Таким образом, в целом все киберпреступления можно условно поделить на две группы – преступления, совершаемые с помощью компьютерных технологий, и «собственно компьютерные преступления». Первая группа включает в себя широкий спектр преступных деяний, которые могут совершаться и без использования компьютера, например, склонение к совершению самоубийства (ст. 110.1 Уголовного кодекса РФ)[3], кража (ст. 158 УК РФ), различные виды мошенничества (ст. 159–159.6 УК РФ) и иные преступления. Вторая группа содержит преступления, которые без компьютеров совершены быть не могут (глава 28 УК РФ). Возвращаясь к определению И. Г. Чекунова, отметим, что вторым его недостатком является указание на вредоносность программ, используемых при совершении киберпреступлений. При совершении большого числа мошенничеств при помощи компьютерных технологий каких-либо вредоносных программ не применяется[4].

Более верным нам видится определение киберпреступности, которое предлагает Т. Л. Тропина, – под киберпреступностью понимается совокупность преступлений, совершаемых в киберпространстве с помощью или посредством компьютерных систем или компьютерных сетей, а также иных средств доступа к киберпространству в рамках

---

[1] Чекунов И. Г. Криминологическое и уголовно-правовое обеспечение предупреждения киберпреступности: автореф. дис. ... канд. юрид. наук. М., 2013. С. 7.

[2] Kranenbarg M. W., Ruiter S., Van Gelder J.-L. Do cyber-birds flock together? Comparing deviance among social network members of cyber-dependent offenders and traditional offenders // European Journal of Criminology. URL: https://journals.sagepub.com/doi/full/10.1177/1477370819849677 (дата обращения: 29.12.2020).

[3] См.: Минаева Е. В. Склонение к самоубийству с использованием сети Интернет: опасность и правовая оценка // Центр защиты прав и интересов детей: сайт. 2020. URL: https://fcprc.ru/wp-content/uploads/2019/05/Modul-4.-Sklonenie-k-samoubijstvu-s-ispolzovniem-seti-internet-Minaeva-E.V..pdf (дата обращения: 30.12.2020).

[4] См.: Интернет-мошенничество – памятка для граждан // Министерство внутренних дел РФ: официальный сайт. 2020. URL: https://мвд.рф/document/1910260 (дата обращения: 30.12.2020).

компьютерных систем или сетей и против компьютерных систем, компьютерных сетей и компьютерных данных[1]. В данном определении также содержится указание на средство совершения киберпреступлений, однако акцент смещается на «место» совершения таких преступлений – киберпространство.

Более лаконичное, но от этого не менее точное определение можно встретить в зарубежной литературе. Киберпреступность охватывает широкий спектр действий, связанных с использованием информационных технологий в преступных целях[2]. Однако в данном определении опять-таки делается упор на средства совершения киберпреступлений. Определение киберпреступлений как преступных или вредоносных действий, которые носят информационный, глобальный и сетевой характер и акцент на их в отличии от преступлений, в которых просто используются компьютеры, более точно[3]. Таким образом, киберпреступления можно определить как деяния, совершаемые в киберпространстве или с использованием компьютерных технологий, и наносящие вред законным правам и интересам физических и юридических лиц, а также государства.

Динамика киберпреступлений показывает беспрецедентный рост. В 2017 году[4] было зарегистрировано 90 587 преступлений, в 2018 – 174 674 преступления (+92,8 % по сравнению с 2017), в 2019 – 294 409 (+68,5 % по сравнению с 2018), а за январь–октябрь 2020 – 420 662 (+75,1 % по сравнению с январем–октябрем 2019 года)[5]. При этом одним из характерных признаков киберпреступлений является довольно низкий процент раскрываемости. По данным Европейского общества криминологов, средняя раскрываемость «обычных» преступлений составляет 42–46 %, а киберпреступлений – 5 %[6]. В России

[1] Тропина Т. Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы: автореф. дис. ... канд. юрид. наук. Владивосток, 2005. С. 9.

[2] Rush H., Smith C., Kraemer-Mbula E., Tang P. Crime online: Cybercrime and illegal innovation (research report: July 2009) // ResearchGate: site. 2020. URL: https://www.researchgate.net/publication/28550926_Crime_Online_Cybercrime_and_illegal_innovation (дата обращения: 30.12.2020).

[3] Rush H. Op. cit. P. 11.

[4] Необходимо отметить, что строка «[количество преступлений], совершенных с использованием компьютерных и телекоммуникационных технологий» появилась в статистических сборниках МВД только в 2017 году.

[5] Состояние преступности // Министерство внутренних дел РФ: официальный сайт. 2020. URL: https://мвд.рф/folder/101762 (дата обращения: 30.12.2020).

[6] Гилинский Я. И. Человеческое, слишком человеческое. СПб.: Изд-во Алетейя, 2020. С. 71.

раскрываемость несколько выше[1]: по данным МВД РФ, за 2017 год было раскрыто 20 424 преступления (22,5 % от числа зарегистрированных за 2017 года), в 2018 году раскрыто 43 362 преступления (24,8 % от числа зарегистрированных), в 2019 году раскрыто 65 238 преступлений (22,1 % от числа зарегистрированных), а за январь–октябрь 2020 года раскрыто 77 357 преступлений (18,4 % от числа зарегистрированных)[2]. К тому же следует помнить про высокую латентность киберпреступлений.

Для повышения эффективности противодействия киберпреступности в структуре МВД РФ будет создано специальное подразделение – киберполиция[3]. Вместе с тем необходимо также учитывать и особенности виктимологической характеристики жертв киберпреступлений, чтобы на ее основе выстраивать эффективную предупреждающую политику. Wytskevander Wagen и Wolter Pieters отмечают, что для киберпреступлений характерен несколько иной подход к характеристике жертвы. Они предлагают концепт victimcomposition, с точки зрения которого жертва рассматривается как совокупность человека, технических и виртуальных объектов[4].

Кроме того, нельзя не отметить и некоторые различия в уголовном законодательстве России и западных стран. На Западе уголовно преследуется «троллинг»[5], харассмент и кибербуллинг, стокерство (или сталкерство)[6]. Хотя в России также содержатся уголовно-правовые запреты, направленные на охрану тайны личной жизни, недопущение распространения клеветы, однако статистика показывает, что основные усилия

---

[1] Впрочем, здесь следует учитывать и высокую латентность, в том числе искусственную, и особенности отечественной статистики (см.: Гилинский Я. И. Криминология: теория, история, эмпирическая база, социальный контроль. Авторский курс. СПб.: ООО Издательский Дом «Алеф-Пресс», 2018. С. 54–55).

[2] Состояние преступности // Министерство внутренних дел РФ: официальный сайт. 2020. URL: https://мвд.рф/folder/101762 (дата обращения: 30.12.2020).

[3] В структуре МВД создается киберполиция // Российская Газета: сайт. 2020. URL: https://rg.ru/2020/12/18/v-strukture-mvd-sozdaetsia-kiberpoliciia.html (дата обращения: 30.12.2020).

[4] Van der Wagen W., Pieters W. The hybrid victim: Re-conceptualizing high-tech cyber victimization through actor-network theory // European Journal of Criminology. URL: https://journals.sagepub.com/doi/full/10.1177/1477370818812016 (дата обращения: 30.12.2020).

[5] См.: What is online trolling, is it a crime and was Brenda Leyland trolling the parents of Madeleine McCann? // INDEPENDENT: site. 2020. URL: https://www.independent.co.uk/news/uk/home-news/what-online-trolling-it-crime-and-was-brenda-leyland-trolling-parents-madeleine-mccann-9777230.html (дата обращения: 30.12.2020).

[6] Cyber /onlinecrime // CPS: site. 2020. URL: https://www.cps.gov.uk/crime-info/cyber-online-crime (дата обращения: 30.12.2020).

правоохранительных органов сосредоточены на недопущении оскорбления представителей власти и государственных символов[1].

Таким образом, киберпреступность является новым, очень опасным явлением, для которого к тому же характерны высокая латентность и низкая раскрываемость. Все это обусловливает необходимость поиска эффективных решений противодействия киберпреступности.

Список литературы

1. В структуре МВД создается киберполиция // Российская Газета: сайт. 2020. URL: https://rg.ru/2020/12/18/v-strukture-mvd-sozdaetsia-kiberpoliciia.html (дата обращения: 30.12.2020).
2. Гилинский Я. И. Человеческое, слишком человеческое. СПб.: Изд-во Алетейя, 2020.
3. Состояние преступности // Министерство внутренних дел РФ: официальный сайт. 2020. URL: https://мвд.рф/folder/101762 (дата обращения: 30.12.2020).
4. Тропина Т. Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы : автореф. дис. ... канд. юрид. наук. Владивосток, 2005.
5. Чекунов И. Г. Криминологическое и уголовно-правовое обеспечение предупреждения киберпреступности: автореф. дис. ... канд. юрид. наук. М., 2013.
6. Cyber / onlinecrime // CPS: site 2020. URL: https://www.cps.gov.uk/crime-info/cyber-online-crime (дата обращения: 30.12.2020).
7. Goldsmith A., Wall D. S. The seduction of cybercrime: Adolescence and the thrills of digital transgression // European Journal of Criminology. URL: https://journals.sagepub.com/doi/full/10.1177/1477370819887305 (дата обращения: 29.12.2020).
8. Internet usage statistics. The Internet Big Picture. World Internet Users and 2020 Population Stats // Internet World Stats: Usage and Population Statistics. 2020. URL: https://www.internetworldstats.com/stats.htm (дата обращения: 29.12.2020).
9. Kranenbarg M. W., Ruiter S., Van Gelder J.-L. Do cyber-birds flock together? Comparing deviance among social network members of cyber-dependent offenders and traditional offenders // European Journal of Criminology. URL: https://journals.sagepub.com/doi/full/10.1177/1477370819849677 (дата обращения: 29.12.2020).
10. Rush H., Smith C., Kraemer-Mbula E., Tang P. Crime online: Cybercrime and illegal innovation (research report: July 2009) // ResearchGate: site. 2020. URL: https://www.researchgate.net/publication/28550926_Crime_Online_Cybercrime_and_illegal_innovation (дата обращения: 30.12.2020).
11. Van der Wagen W., Pieters W. The hybrid victim: Re-conceptualizing high-tech cyber victimization through actor-network theory // European Journal of Criminology. URL: https://journals.sagepub.com/doi/full/10.1177/1477370818812016 (дата обращения: 30.12.2020).

[1] См.: Оскорбление российских госсимволов рассмотрит Страсбургский суд // Коммерсантъ: сайт. 2020. URL: https://www.kommersant.ru/doc/4093972 (дата обращения: 30.12.2020); За оскорбление представителей власти осуждены более 10 тысяч человек // Российская Газета: сайт. 2020. URL: https://rg.ru/2020/05/17/za-oskorblenie-predstavitelej-vlasti-osuzhdeny-bolee-10-tysiach-chelovek.html (дата обращения: 30.12.2020).

Н. Н. Сысоева

АКТУАЛЬНЫЕ ВОПРОСЫ ПРОТИВОДЕЙСТВИЯ КИБЕРСТАЛКИНГУ СРЕДИ НЕСОВЕРШЕННОЛЕТНИХ В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ ИНТЕРНЕТ

Аннотация: В настоящей статье затронуты наиболее актуальные вопросы, связанные с предупреждением и пресечением кибersталкинга среди несовершеннолетних в информационно-телекоммуникационной сети Интернет. Рассмотрены основные паттерны, определяющие кибersталкинг как современную форму противоправного поведения в Сети. Проработаны и предложены пути по совершенствованию действующего административного и уголовного законодательства в сфере противодействия социально-психологической травле в Сети.

Ключевые слова: кибербуллинг, кибersталкинг, информационно-телекоммуникационная сеть Интернет, девиантная субкультура.

TOPICAL ISSUES OF COUNTERING CYBERSTALKING AMONG MINORS IN THE INFORMATION AND TELECOMMUNICATIONS NETWORK INTERNET

Abstract: This article touches upon the most pressing issues related to the prevention and suppression of cyberstalking in the information and telecommunications network Internet; the main patterns that define cyberstalking as a modern form of illegal behavior in the network are considered; developed and proposed ways to improve the current administrative and criminal legislation in the field of countering social and psychological harassment in the network.

Keywords: cyberbullying, cyberstalking, information and telecommunications network Internet, deviant subculture.

Информационно-телекоммуникационная сеть Интернет является наиболее доступным средством не только для получения необходимой информации или обучения, но и для совершения противоправных действий.

В последнее время одним из наиболее распространенных правонарушений, оказывающих существенное влияние на психическое здоровье подростков, выступает кибersталкинг. Феномены кибербуллинга и кибersталкинга вот уже многие годы являются предметом исследований, проводимых отечественными и зарубежными криминологами.

Рассмотрим подробнее общественную опасность и противоправность указанных действий.

При кибербуллинге основное внимание правонарушителей сосредотачивается на осуществлении фактического давления на потенциальную

жертву. При этом указанное давление может выражаться как прямо, так и косвенно в устной, письменной форме или конклюдентно (путем осуществления демонстрации или использования различных фото-, видеоматериалов). Зачастую подобные противоправные действия в виртуальном пространстве могут сопровождаться действиями шуточно-уничижительного характера (например, «пранк», «троллинг»), в том числе и с распространением соответствующих аудиоматериалов в широком доступе.

Осуществляя противоправные действия, правонарушитель может запугивать жертву, угрожать ей, преследуя тем самым собственные низменные, корыстные цели или реализуя патологическое стремление к всеобщему вниманию.

Кибersталкинг, в свою очередь, представляет собой преследование какого-либо лица в интернет-пространстве и других информационно-телекоммуникационных сетях.

Кибersталкинг сопровождается сбором информации о жертве посредством использования доступных правонарушителю информационно-поисковых систем, нелегального программного обеспечения (в том числе посредством хакер-атак, фишинга), с последующим привлечением внимания интернет-пользователей, сообществ к личности потерпевшего лица, интерпретируя полученные личные сведения о нем в негативном ключе. Одним из распространенных способов кибersталкинга является фактическое унижение жертвы в сети Интернет путем форсированного распространения информации о ней через различные чаты, форумы, блоги, топики, интернет-страницы, социальные сети и медиаресурсы (например, TikTok, Likee). Проявления подобного вида сталкинга включают в себя различные виды угроз и имеют своей целью довести жертву до истощения от нервного перенапряжения, а, иногда и до возможного самоубийства.

Особую «популярность» данное явление приобрело среди несовершеннолетних. В настоящее время жертвой кибersталкинга может стать любой подросток, активно пользующийся техническими ресурсами и современными средствами обмена информацией и связи.

При осуществлении киберпреследования правонарушителем используется абсолютно любой повод, даже надуманный. При этом среди несовершеннолетних правонарушителей какой-либо повод может и вовсе отсутствовать. Нередко кибербуллинг и кибersталкинг используются подростками для сведения счета с кем-либо в ситуации ревности (девушки «не поделили» молодого человека), зависти (жертва более

успешна в учебе или материально благополучна), в качестве способа наказать, отыграться, показать свои значимость, величие и одновременно безнаказанность.

По данным ВОЗ, ежегодно социальным преследованиям в России (в том числе и в киберпространстве) подвергаются до 20 % детей в возрасте от 10 до 12 лет, 19 % – от 13 до 14 лет, 13 % подростков от 15 до 18 лет[1].

Основным проявлением кибersталкинга является активное психологическое влияние на человека, которое по характеру воздействия, оказываемого на потерпевшего, безусловно, может расцениваться как насилие. Нередко бывают случаи, когда психическое насилие при кибersталкинге может привести к серьезным последствиям для ментального здоровья потерпевшего. Жертва насилия становится замкнутой, проявляет сложности в социализации, общении, резко меняет сферу интересов, нередко погружается в виртуальную среду, в том числе начинает интересоваться запрещенным или специфическим контентом (пропагандирующим насилие, радикальные религиозные воззрения, суициды и пр.). Иногда изменения в поведении несовершеннолетней жертвы заметить трудно, что может быть обусловлено трудностями в социализации подростка, боязнью выразить недовольство и нарекания со стороны родителей, быть неверно понятыми или презираемыми окружающими и обществом.

С развитием современных информационных технологий анонимного пользователя-сталкера (или пользователей) в Сети вычислить стало гораздо проще, однако каких-либо реальных правовых последствий в большинстве случаев для виновных лиц не наступает – в основном из-за возраста правонарушителей (максимум – постановка на профилактический учет в подразделениях по делам несовершеннолетних за совершение антиобщественных действий сроком на 1 год) или отсутствия видимых общественно-опасных последствий (в 70 % случаев при обращении жертв кибersталкинга в правоохранительные органы при отсутствии тяжких последствий указанных действий в возбуждении уголовного дела отказывается за отсутствием состава или события преступления).

При этом не секрет, что потерпевшие, особенно подростки, очень тяжело переживают кибersталкинг, когда публикации в открытом доступе начинают активно обсуждать, из-за чего у жертвы кибersталкинга может

[1] Издевательства среди детей: что такое буллинг и почему он опасен для ребенка. URL: https://news.yellmed.ru/deti/izdevatelstva-sredi-detey-chto-takoe-bulling-i-pochemu-on-mozhet-byt-opasen-dlya-rebenka (дата обращения: 19.12.2020).

развиться вполне психофизиологическая, а не виртуальная (гипотетическая) мания преследования.

Кибersталкинг в условиях тотальной глобализации стал приобретать массовый характер. Кибersталкеры с целью систематического поиска и унижения своих потенциальных жертв объединяются в референтные группы, а порой и контекстные сообщества. Идентификация членов подобных групп и сообществ в многопользовательском режиме существенно затруднена, так как требует значительных временных и ресурсных затрат, в результате чего указанные объединения начинают приобретать статус устоявшихся, а явление – статус субкультуры.

В связи с этим необходимо выделить несколько путей решения обозначенных проблем.

Во-первых, самая действенная помощь для подростка в случае кибersталкинга – это разговоры со взрослыми. Родителям необходимо больше внимания уделять ребенку, понимать, в каком состоянии он находится и как именно он взаимодействует со сверстниками посредством сети Интернет. Это касается не только родителей (законных представителей), но также и педагогов-психологов, работников образовательных учреждений, сотрудников правоохранительных органов и иных субъектов профилактики.

Во-вторых, целесообразно ввести отдельный вид юридической ответственности за кибersталкинг, а именно:

- выделить новый вид административно-правовых норм, предусматривающих административную ответственность за «унижение человеческого достоинства, выразившееся в преследовании потерпевшего в сети Интернет», которую отнести к группе правонарушений, посягающих на общественный порядок, выделив особым составом, введя статью 20.1.1 в КоАП РФ. В качестве квалифицирующего признака обозначить ответственность за «совершение указанных действий в отношении несовершеннолетних».
- УК РФ дополнить статьей 110.3 «Склонение к самоубийству, если эти действия сопряжены с унижением человеческого достоинства, выразившимся в преследовании потерпевшего в сети Интернет», выделив в качестве отдельных признаков: «повторное совершение административного правонарушения, выразившегося в унижении человеческого достоинства, посредством преследования потерпевшего в сети Интернет

в течение срока, когда лицо считалось подвергнутым административному наказанию», «совершение указанных действий в отношении несовершеннолетнего, чей возраст известен или очевиден виновному» и «преступление, совершенное в группе лиц, группе лиц по предварительному сговору или организованной группой» (данное решение небезосновательно, так как направлено на борьбу с «сообществами кибersталкеров», одной из целей которых являются пропаганда взглядов и продвижение идеологии кибersталкерства как одного из видов девиантных субкультур в современном обществе). Составы по конструкции материальной стороны предлагаем считать формальными.

В заключение хотелось бы отметить, что общественная опасность кибersталкинга в условиях цифровизации общественных отношений реальна как никогда, и необходимость поиска оптимальных путей его предупреждения является одной из первоочередных задач современного законодательства.

Своевременное пресечение подобных проявлений позволит осуществлять профилактику подростковых суицидов и существенно снизить уровень противоправного поведения в Сети.

Список литературы

1. Вихляев А. А. О некоторых проблемах, возникающих при выявлении и пресечении правонарушений, совершаемых несовершеннолетними // Актуальные вопросы административной деятельности полиции. Сборник научных трудов. М., 2019. С. 30–36.
2. Макарова Е. А. Психологические особенности кибербуллинга как формы интернет-преступления // Российский психологический журнал. М., 2016. № 3. С. 293–311.

А. А. Цибульская

ПРОТИВОДЕЙСТВИЕ КАРТЕЛЯМ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ

Аннотация: Цифровизация тендеров, с одной стороны, способствует их прозрачности, но в тоже время переход на электронную форму закупок привел к появлению новых рисков – неправомерному использованию цифровых технологий в рассматриваемой сфере и необходимости пересмотра статуса конституционно охраняемой информации.

Ключевые слова: государственная закупка, картель, конкуренция, торги, IT-технологии.

COUNTERING CARTELS IN THE CONTEXT OF DIGITALIZATION

Abstract: Digitalization of tenders, on the one hand, contributes to its transparency. But at the same time, the transition to the electronic form of procurement led to the emergence of new risks - the illegal use of digital technologies in this area and the need to revise the status of constitutionally protected information.

Keywords: public procurement, cartel, competition, bidding, IT-technologies.

Современную жизнь характеризуют цифровизация и активное внедрение IT-технологий в сферу государственных и муниципальных закупок, которую некоторые специалисты справедливо относят к одной из наиболее развитых «цифровых сфер в России…»[1]. Но, как и любое социальное явление, оно содержит в себе новые возможности и новые угрозы.

С 2008 года согласно распоряжению Правительства России размещение заказов на поставки товаров, выполнение услуг и т. п. может производиться только путем проведения открытых аукционов в электронной форме[2].

Первые электронные торговые площади (ЗАО «Сбербанк-АСТ», ООО «РТС-тендер», ОАО «Единая электронная торговая площадка», ГУП «Агентство по государственному заказу Республики Татарстан»,

[1] Актуальные вопросы современного конкурентного права: сборник научных трудов / Д. М. Ашфа, И. В. Башлаков-Николаев, О. А. Беляева и др.; отв. ред. М. А. Егорова. М.: Юстицинформ, 2019. Вып. 3 // СПС «Консультант Плюс».

[2] См.: Распоряжение Правительства РФ от 27.02.2008 № 236-р (документ утратил силу) «О перечне товаров (работ, услуг), размещение заказов на поставки (выполнение, оказание) которых осуществляется путем проведения аукциона» // СЗ РФ. 03.03.2008. № 9. ст. 884.

а также ЗАО «Московская межбанковская валютная биржа») для государственных и муниципальных нужд были отобраны и утверждены еще в 2009 году[1].

Как следствие подобного решения возникли проблемы противодействия неправомерным сговорам на торгах, поскольку основным требованиям к заявкам является их анонимность. Предполагается, что участники торгов не должны знать друга, и это положение должно было стать препятствием для создания и вступления в картельное соглашение. Но уже в 2011 году ФАС России возбудил первое дело, в котором в качестве доказательства явилось использование участниками картеля одного IP-адреса[2]. В настоящее время, по данным ФАС РФ, ежегодно возбуждается около 400 дел, из них около 85 % –сговоры на торгах[3].

В этой связи ФАС России разработала очередной, пятый, пакет о внесении изменений в Закон о защите конкуренции, обратив особое внимание на необходимость регулирования отношений в сфере цифровых технологий. В 2019 году была принята Межведомственная целевая программа мер по выявлению и пресечению картелей и иных, ограничивающих конкуренцию, соглашений на 2019–2023 годы[4]. В 2020 году в рамках распоряжения Правительства России от 17.06.2019 года № 1314-р ФАС России подготовил специальные методические рекомендации, посвященные выявлению цифровых антимонопольных сговоров[5].

Но в целом необходимо признать, что до сих пор практика противодействия данному явлению отсутствует. Хотя определенные шаги и делаются.

В частности, был разработан так называемый «Большой цифровой кот» – программное обеспечение, которое позволяет в онлайн-режиме

---

[1] Приказ Минэкономразвития России от 26.10.2009 № 428 «Об утверждении Порядка отбора электронных площадок в целях проведения открытых аукционов в электронной форме» // Российская газета, № 208, 03.11.2009.

[2] Решение ФАС России от 06.04.2012 № АЦ/10491 по делу № 1 11/141-11 о нарушении антимонопольного законодательства.

[3] Картели: итоги работы ФАС России за 2017 год и планы на 2018 год. Интернет-интервью с А. П. Тенишевым, начальником Управления по борьбе с картелями ФАС России // СПС «Консультант Плюс».

[4] Распоряжение Правительства России от 17.06.2019 года № 1314-р «Межведомственная программа мер по выявлению и пресечению картелей и иных ограничивающих конкуренцию соглашений на 2019–2023 годы». URL: https://www.garant.ru/products/ipo/prime/doc/72180706/ (дата обращения: 11.01.2020).

[5] Опубликованы методические рекомендации по выявлению картелей в условиях цифровой экономики. URL: https://fas.gov.ru/news/30139 (дата обращения: 15.01.2021).

выявлять признаки антиконкурентных соглашений на торгах и создавать доказательственную базу. Но при этом «антимонопольный орган пока не обладает возможностью дополнительно квалифицировать такие действия в соответствии с Законом о защите конкуренции и использует полученную информацию исключительно в целях доказывания факта заключения и участия в антиконкурентных соглашениях»[1].

УК РФ содержит составы преступления, которые в определенной степени могут охватывать действия недобросовестных участников торгов. Это могут быть ст. 272 УК РФ («Неправомерный доступ к компьютерной информации»), ст. 273 УК РФ («Создание, использование и распространение вредоносных компьютерных программ») и ст. 274 УК РФ («Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей»).

Но следует сразу согласиться с А. П. Тенишевым и А. В. Тесленко, которые справедливо указывают, что «указанными нормами не охватываются все возможные случаи цифрового ограничения конкуренции и требуется дополнительное исследование вопросов, связанных с цифровыми рисками закупочной деятельности, в целях выработки оптимального варианта уголовно-правового реагирования на такие действия»[2].

Действительно, в одних случаях действия участников цифровых картелей охватываются ст. 178 УК РФ и не требуют дополнительной квалификации, в других – они могут охватываться совокупностью ст. 178 и 273 (или ст. 178 и 272, ст. 178 и 274), либо вообще не могут быть квалифицированы как преступления.

Проблема противодействия картелям в условиях цифровой экономики осложняется еще и тем, что существует целый ряд установленных законом иммунитетов, которые в настоящее время ФАС России пытается преодолеть. В результате в научной среде и между правоприменителями ведется дискуссия о границах антимонопольного права, возможности расширения полномочий ФАС России в данной сфере. В частности, о доступе в процессе контроля за торгами за IP-адресами участников торгов, статусе конституционно охраняемой информации и т. д. И хотя защита персональных данных и защита конкуренции – два самостоятельных понятия и две не связанные между собой сферы правового

[1] Тенишев А. П., Тесленко А. В. Уголовно-правовая охрана конкуренции в условиях развития цифровых технологий // Закон. 2019. № 6. С. 124–131.

[2] Тенишев А. П., Тесленко А. В. Уголовно-правовая охрана конкуренции в условиях развития цифровых технологий // Закон. 2019. № 6. С. 124–131.

регулирования, но для преодоления рисков, сопряженных с неправомерным использованием цифровых технологий во время торгов, обществу необходимо выработать определенный баланс интересов личности, бизнеса, конкуренции и монополизма.

Список литературы

1. Приказ Минэкономразвития России от 26.10.2009 № 428 «Об утверждении Порядка отбора электронных площадок в целях проведения открытых аукционов в электронной форме» // Российская газета. № 208. 03.11.2009.
2. Распоряжение Правительства России от 17.06.2019 года № 1314-р «Межведомственная программа мер по выявлению и пресечению картелей и иных ограничивающих конкуренцию соглашений на 2019–2023 годы». URL: https://www.garant.ru/products/ipo/prime/doc/721807 (дата обращения: 11.01.2021).
3. Распоряжение Правительства РФ от 27.02.2008 № 236-р (документ утратил силу) «О перечне товаров (работ, услуг), размещение заказов на поставки (выполнение, оказание) которых осуществляется путем проведения аукциона» // СЗ РФ. 03.03.2008. № 9. ст. 884.
4. Картели: итоги работы ФАС России за 2017 год и планы на 2018 год. Интернет-интервью с А. П. Тенишевым, начальником Управления по борьбе с картелями ФАС России // СПС «Консультант Плюс».
5. Опубликованы методические рекомендации по выявлению картелей в условиях цифровой экономики. URL: https://fas.gov.ru/news/30139 (дата обращения: 15.01.2021).
6. Решение ФАС России от 06.04.2012 № АЦ/10491 по делу № 1 11/141-11 о нарушении антимонопольного законодательства.
7. Актуальные вопросы современного конкурентного права: сборник научных трудов / Д. М. Ашфа, И. В. Башлаков-Николаев, О. А. Беляева и др.; отв. ред. М. А. Егорова. М.: Юстицинформ, 2019. Вып. 3 // СПС «Консультант Плюс».
8. Тенишев А. П., Тесленко А. В. Уголовно-правовая охрана конкуренции в условиях развития цифровых технологий // Закон. 2019. № 6. С. 124–131.

А. М. Яблоков

ПУБЛИЧНЫЙ ИНТЕРНЕТ-РЕЕСТР (ПИР) В КАЧЕСТВЕ ИНСТРУМЕНТА ВЗАИМОДЕЙСТВИЯ ОБЩЕСТВА И ГОСУДАРСТВА В РАМКАХ ОРГАНИЗАЦИИ ПРОЦЕССА КОНТРОЛЯ НАД ПРЕСТУПНОСТЬЮ

Аннотация: Увеличение киберпреступлений является обстоятельством, требующим принятия мер, направленных на «усмирение» этого явления. Обосновывается необходимость создания публичного интернет-реестра на территории Российской Федерации, который может быть внедрен и в других странах, став российской разработкой в сфере осуществления контроля над киберпреступностью.

Ключевые слова: публичный интернет-реестр (ПИР), киберпреступность, предупреждение преступности.

PUBLIC INTERNET REGISTER (PIR) AS A TOOL FOR INTERACTION BETWEEN SOCIETY AND THE STATE IN THE FRAMEWORK OF ORGANIZING THE PROCESS OF CRIME CONTROL

Abstract: The increase in cybercrime is a circumstance that requires the adoption of measures aimed at "taming" this phenomenon. The article substantiates the need to create a public Internet registry on the territory of the Russian Federation, which can be implemented in other countries, becoming a Russian development in the field of control over cybercrime.

Keywords: public internet registry (PIR), cybercrime, crime prevention.

В 2019 году доля интернет-торговли на российском рынке составила 6,1 %[1]. Непосредственно рост интернет-торговли составил 18 % по сравнению с прошлым 2018 годом. На тот момент основной причиной увеличения присутствия интернет-продаж на рынке специалисты НИУ ВШЭ называли привыкание потребителя к интернет-покупкам в силу улучшения качества интернет-площадок.[2] При этом уже в декабре 2019 года, в период фиксации первых случаев заболевания вирусом COVID-19, имелись предположения о том, что в случае ухудшения ситуации (что и произошло позднее) интернет-торговлю ожидает прирост. В первом же полугодии 2020 года доля интернет-торговли на российском рынке выросла до 10 %.

[1] Российский рынок интернет-торговли: итоги 2019 года, тренды 2020-го. НИУ ВШЭ. URL: https://www.hse.ru/mirror/pubs/share/373094071.pdf (дата обращения: 15.01.2021).

[2] Доля онлайна в российской рознице приблизилась к уровню развитых стран // РБК. 10.09.2020. URL: https://www.rbc.ru/rbcfreenews/5f592c909a79471b55995534. (дата обращения: 15.01.2021).

Самоизоляция (из-за COVID-19) фактически заставила общество приобщаться к работе «на удаленке» со всеми сопутствующими «удобствами». Но насколько рациональными являются меры, предпринятые государством для защиты здоровья общества, покажут время и статистика. С самого начала пандемии стало очевидным то, что жизнедеятельность общества поменялась, корректировке подвергся не только механизм удовлетворения личных потребностей, но и сама жизнедеятельность общества (и каждого члена общества в отдельности) «сдвинулась» в сторону киберпространства.

Учитывая, что COVID-19 – это не локальная, но глобальная проблема, которая коснулась всех без исключения, потерпевшим от вируса стал и преступный контингент, который также рассеялся, уйдя с улиц на «просторы киберполя».

Уже к июлю 2020 года количество разбоев упало на 23 %, грабежей – на 20 %, краж – на 19,6 %, хищений транспортных средств – на 28,7 %. При этом общее число преступлений снизилось всего на 0,1 %[1].

Однако стоит отметить, что «насовсем» преступность в киберпространство не ушла. Число грабежей и разбоев (самых уличных преступлений) хоть и уменьшилось, но по большей части из-за введения повсеместного режима самоизоляции.

Ведь при условии, когда население не только просыпается и засыпает «по месту жительства», но и трудится там же, находясь при этом в сети Интернет, не использовать это обстоятельство преступник не может. Таким образом, находиться в киберпространстве субъекту преступления в условиях пандемии «удобнее». Безусловно, рано или поздно социальные ограничения будут сняты, и некоторые из субъектов останутся в киберпространстве, но большинство, вероятно, вернутся к «проверенному» способу завладения чужим имуществом, что, конечно, не означает, что обществу стоит ждать, пока уровень киберпреступности снизится самостоятельно, и действовать необходимо незамедлительно.

В ноябре 2020 года Генеральная прокуратура Российской Федерации зафиксировала 461,2 тысячи преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, что в три раза больше, чем в 2018 году. На сегодняшний день каждое четвертое преступление представляется

[1] Улицы стали безопаснее // Российская газета. № 152. 13.07.2020. URL: https://rg.ru/2020/07/13/vopreki-koronavirusnym-opaseniiam-snizilos-chislo-razboev-i-grabezhej.html (дата обращения: 15.01.2021).

возможным отнести к киберпреступлению[1]. К слову, в 2017 году каждое двадцатое преступление относилось к киберпреступлениям.

На сегодняшний день самыми распространенными видами интернет-преступлений являются: «брачные мошенничества», когда денежные средства выманиваются под видом предложения создать «пару»; организация продажи товаров посредством сайтов-одностраничников, схожих с оригинальными сайтами, на которых размещается информация о товарах с весьма привлекательной, но недействительной ценой; «сайты – просьбы о помощи», в действительности не имеющие какого-либо отношения к реальным пациентам медицинских учреждений; спам-рассылки с письмами-приветствиями и просьбами пройти по конкретной ссылке; «брокерские фирмы», завлекающие сильно выгодными условиями инвестирования денежных средств[2].

Стоит отметить, что помимо «памятки для граждан», государство успешно применяет еще один инструмент – блокировку интернет-страниц посредством Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций. Блокировке подвергаются сайты, содержащие информацию: вредную для детей, содержащую детскую порнографию, порнографического характера, о наркотиках, суициде, экстремистского характера, содержащую клевету в сети Интернет, свидетельствующую о нарушении авторских и смежных прав.

Действительно, указанная выше информация является вредной для общества. Однако, помимо выявления и блокировки интернет-сайтов с вредоносной информацией, какие-либо иные инструменты контроля сети Интернет не применяются. Но ведь тот или иной интернет-сайт может непосредственно не содержать вредоносной информации.

При принятии решения о блокировке конкретного интернет-сайта последний рассматривается в качестве «преступного явления» самостоятельно, но в ситуациях с интернет-мошенничеством такие страницы способны выступать в качестве инструмента совершения преступления (составляя объективную сторону преступления) и не являться сами по себе преступными или в перспективе запрещенными. Ведь маловероятно, что тот или иной «сайт знакомств» подвергнется блокировке, если в случае «знакомства» посредством такого сайта субъект преступления

[1] Генеральная прокуратура Российской Федерации. Состояние преступности в России за январь–ноябрь 2020 года. М., 2020. С. 6.

[2] Министерство внутренних дел Российской Федерации. Интернет-мошенничество – памятка для граждан. URL: https://xn--b1aew.xn--p1ai/document/1910260. (дата обращения: 15.01.2021).

доведет свой умысел до конца, похитив денежные средства (или информацию) у объекта преступления. Также будут ли иметься основания блокировки того или иного «мессенджера» или почтового сервиса, в рамках которого пользователи ежедневно получают спам-рассылки? Или как много потребуется времени для того чтобы установить действительность наличия физического недуга у пациента, от имени которого публикуются просьбы о помощи, которые представляется возможным нередко наблюдать на интернет-страницах? И возможно ли запретить кому-либо предлагать приобрести товар по «удивительно выгодной цене», когда имеет место быть свобода договора.

Проблема проникновения в «личное цифровое пространство» является актуальной проблемой, усугубляясь тем, что взаимоотношения интернет-контрагентов не всегда возможно проследить вплоть до физических лиц. Интернет-контрагентов «бесконечное» множество, но терять контроль представляется недопустимым. Решение видится в создании Публичного интернет-реестра (ПИР – публичный интернет-реестр, PIR – public internet registry, термин вводится автором).

При этом реестров информационного характера на территории Российской Федерации немало: единый государственный реестр юридических лиц, единый государственный реестр недвижимости, государственный реестр цен на жизненно необходимые и важнейшие лекарственные средства, реестр средств массовой информации, единый государственный реестр лотерей и др.

С 1 января 2017 года на территории России Федеральным законом «О защите прав и законных интересов физических лиц при осуществлении деятельности по возврату просроченной задолженности и о внесении изменений в Федеральный закон «О микрофинансовой деятельности и микрофинансовых организациях»» от 03.07.2016 № 230-ФЗ как форма учета принят государственный реестр юридических лиц, осуществляющих деятельность по возврату просроченной задолженности в качестве основного вида деятельности. Одной из главных причин введения указанного реестра явилось наличие необходимости недопущения актуализации взыскания долгов «в стиле 90-х». Введение реестра встретило положительные отзывы[1].

Публичный интернет-реестр, как представляется, должен реализовать процесс аккумулирования максимально объективной информации

[1] «Выиграют все». Юристы оценили создание реестра легальных коллекторских агентств. 18 января 2017 года. URL: https://pravo.ru/news/view/137301/ (дата обращения: 18.01.2021).

относительно деятельности интернет-контрагентов, предоставляющих услуги и (или) товары пользователям сети Интернет, а также относительно противоправной деятельности как физических, так и юридических лиц, совершающих деяния посредством использования сети Интернет. Публичный интернет-реестр должен обеспечить интернет-пользователей возможностью осуществлять самостоятельный контроль за «общественным уровнем доверия» к тем или иным интернет-контрагентам в процессе выстраивания взаимоотношений, что позволит сделать такие взаимоотношения более «прозрачными». Учитывая, что в рамках публичного интернет-реестра сама общественность будет иметь возможность фиксировать нарушения, «принцип прозрачности» представляется возможным соблюдать в действительности.

Кроме того, публичный интернет-реестр должен упростить процесс взаимодействия общества и государства в рамках осуществления контроля над преступностью. Формы, бланки, которые предусмотрены теми или иными ведомствами, зачастую представляются сложными к осознанию гражданами, и публичный интернет-реестр позволит реагировать в первую очередь на содержание, а не на форму обращения, что важно при наличии весьма невысокого уровня правовой грамотности населения нашей страны[1].

Список литературы

1. «Выиграют все». Юристы оценили создание реестра легальных коллекторских агентств. 18 января 2017 года. URL: https://pravo.ru/news/view/137301/ (дата обращения: 18.01.2021).
2. Генеральная прокуратура Российской Федерации. Состояние преступности в России за январь–ноябрь 2020 года. М., 2020.
3. Министерство внутренних дел Российской Федерации. Интернет-мошенничество – памятка для граждан. URL: https://xn--b1aew.xn--p1ai/document/1910260 (дата обращения: 15.01.2021).
4. Российский рынок интернет-торговли: итоги 2019 года, тренды 2020- го // НИУ ВШЭ. URL: https://www.hse.ru/mirror/pubs/share/373094071.pdf (дата обращения: 15.01.2021).
5. Паутина Е. Ю. Немного о правовой грамотности // Актуальные проблемы права: материалы V Междунар. науч. конф. (г. Москва, декабрь 2016 года). М., 2016. С. 7–9.
6. Доля онлайна в российской рознице приблизилась к уровню развитых стран // РБК. 10.09.2020. URL: https://www.rbc.ru/rbcfreenews/5f592c909a79471b55995534 (дата обращения: 15.01.2021).
7. Улицы стали безопаснее // Российская газета. № 152. 13.07.2020. URL: https://rg.ru/2020/07/13/vopreki-koronavirusnym-opaseniiam-snizilos-chislo-razboev-i-grabezhej.html (дата обращения: 15.01.2021).

[1] Паутина Е. Ю. Немного о правовой грамотности // Актуальные проблемы права: материалы V Междунар. науч. конф. (г. Москва, декабрь 2016 года). М., 2016. С. 7–9.

НАШИ АВТОРЫ

Секция 1

- *Баландина Валерия Алексеевна* – студент 1-го курса юридического факультета Северо-Западного филиала ФГБОУВО «Российский государственный университет правосудия». Научный руководитель: Клейменов И. М., профессор кафедры уголовного права Северо-Западного филиала ФГБОУВО «Российский государственный университет правосудия», доктор юридических наук (г. Санкт-Петербург)
- *Бахолдин Олег Игоревич* – студент 3-го курса Института прокуратуры ФГБОУВО «Саратовская государственная юридическая академия». Научный руководитель: Жирнова Н. А., доцент кафедры информационного права Института прокуратуры ФГБОУВО «Саратовская государственная юридическая академия», кандидат юридических наук (г. Саратов)
- *Булавина Мария Романовна* – студент 3-го курса международно-правового факультета Одинцовского филиала ФГАОУВО «Московский государственный институт международных отношений (университет) Министерства иностранных дел Российской Федерации». Научный руководитель: Решняк М. Г., доцент кафедры уголовного права, уголовного процесса и криминалистики международно-правового факультета МГИМО МИД России (Одинцовский филиал), кандидат юридических наук, доцент (г. Москва)
- *Добровольский Дмитрий Денисович* – студент 2-го курса магистратуры юридического института Балтийского федерального университета имени И. Канта. Научный руководитель: Долгова С. В., доцент кафедры уголовного права и криминологии Балтийского федерального университета имени И. Канта, кандидат юридических наук (г. Калининград)
- *Долгополов Александр Александрович* – студент 1-го курса Института публичного права и управления Московской государственной юридической академии. Научный руководитель: Матевосова Е. К., доцент кафедры теории государства и права Университета имени О. Е. Кутафина (МГЮА), кандидат юридических наук, адвокат (г. Москва)

- *Задера Василий Владимирович* – студент 2-го курса Межрегионального юридического института ФГБОУВО «Саратовская государственная юридическая академия». Научный руководитель: Копшева К. О., доцент кафедры уголовно и уголовно-исполнительного права ФГБОУВО «Саратовская государственная юридическая академия», кандидат юридических наук, доцент (г. Саратов)
- *Иващенко Кристина Андреевна* – аспирант ФГБОУВО «Российский государственный университет правосудия». Научный руководитель: Рахманова Е. Н., заведующий кафедрой уголовного права Северо-Западного филиала ФГБОУВО «Российский государственный университет правосудия», доктор юридических наук, доцент (г. Санкт-Петербург)
- *Исмоилова Малика Замировна* – студент факультета международного права и сравнительного правоведения Ташкентского государственного юридического университета. Научный руководитель: Садиков М. А., преподаватель кафедры теории государства и права Ташкентского государственного юридического университета (г. Ташкент, Республика Узбекистан)
- *Карташов Иван Игоревич* – студент 3-го курса юридического факультета Центрального филиала ФГБОУВО «Российский государственный университет правосудия». Научный руководитель: Иванченко Р. Б., заведующий кафедрой уголовного права ЦФ ФГБОУВО «Российский государственный университет правосудия», кандидат юридических наук, доцент (г. Воронеж)
- *Кекко Валерия Сергеевна* – магистрант кафедры уголовного права Северо-Западного филиала ФГБОУВО «Российский государственный университет правосудия». Научный руководитель: Берестовой А. Н., доцент кафедры уголовного права Северо-Западного филиала ФГБОВО «Российский государственный университет правосудия», кандидат юридических наук, доцент (г. Санкт-Петербург)
- *Киракосов Владимир Борисович* – студент 3-го курса юридического факультета ФГАОУВО «Южный федеральный университет». Научный руководитель: Саядова А. С., преподаватель кафедры уголовного права и криминологии ФГАОУВО «Южный федеральный университет» (г. Ростов-на-Дону)
- *Ковтун Карина Александровна* – студент 2-го курса юридического факультета Санкт-Петербургского политехнического университета Петра Великого. Научный руководитель: Липский Н. А., доцент кафедры уголовно-правовых дисциплин Санкт-Петербургского политехнического

университета Петра Великого, кандидат юридических наук (г. Санкт-Петербург)

- *Король Денис Петрович* – магистрант 1-го курса юридического факультета Северо-Западного филиала ФГБОУВО «Российский государственный университет правосудия». Научный руководитель: Краснова К. А., доцент кафедры уголовного права Северо-Западного филиала ФГБОУВО «Российский государственный университет правосудия», кандидат юридических наук, доцент (г. Санкт-Петербург)

- *Лапшова Яна Олеговна* – студент 3-го курса юридического института Самарского национального исследовательского университета имени академика С. П. Королева. Научный руководитель: Мотин О. А., доцент кафедры уголовного права и криминалистики Самарского национального исследовательского университета имени академика С. П. Королева, кандидат юридических наук, доцент (г. Самара)

- *Мазинская Иванна Валерьевна* – студент 4-го курса юридического факультета Северо-Западного филиала ФГБОУВО «Российский государственный университет правосудия». Научный руководитель: Рахманова Е. Н., заведующий кафедрой уголовного права Северо-Западного филиала ФГБОУВО «Российский государственный университет правосудия», доктор юридических наук, доцент (г. Санкт-Петербург)

- *Маньков Максим Александрович* – студент 2-го курса Санкт-Петербургского государственного университета. Научный руководитель: Векленко В. В., профессор кафедры уголовного права Санкт-Петербургского государственного университета, доктор юридических наук, профессор (г. Санкт-Петербург)

- *Павкова Ксения Сергеевна* – студент 3-го курса юридического факультета Санкт-Петербургского юридического института (филиала) Университета прокуратуры РФ. Научный руководитель: Безбородов Д. А., профессор кафедры уголовного права, криминологии и уголовно-исполнительного права Санкт-Петербургского юридического института (филиала) Университета прокуратуры Российской Федерации, кандидат юридических наук, доцент, старший советник юстиции (г. Санкт-Петербург)

- *Поспех Роман Олегович* – студент 2-го курса магистратуры Юридического института ФГБОУВО «Иркутский государственный университет». Научный руководитель: Сутурин М. А., доцент кафедры уголовного права ФГБОУВО «Иркутский государственный университет», кандидат юридических наук (г. Иркутск)

- *Потапова Софья Сергеевна* – студент 3-го курса Санкт-Петербургского юридического института (филиала) Университета прокуратуры Российской Федерации. Научный руководитель: Безбородов Д. А. профессор кафедры уголовного права, криминологии и уголовно-исполнительного права Санкт-Петербургского юридического института (филиала) Университета прокуратуры Российской Федерации, кандидат юридических наук, доцент, старший советник юстиции (г. Санкт-Петербург)
- *Спехова Ксения Александровна* – студент 3-го курса юридического факультета Санкт-Петербургского института (филиала) ВГУЮ (РПА Минюста России). Научный руководитель: Зорин А. В., доцент кафедры уголовного права и процесса Санкт-Петербургского института (филиала) ВГУЮ (РПА Минюста России), кандидат юридических наук (г. Санкт-Петербург)
- *Терехов Максим Геннадьевич* – инспектор отдела международного сотрудничества Московского университета МВД России имени В. Я. Кикотя. Научный руководитель: Тумаков А. В., начальник кафедры гражданского и трудового права, гражданского процесса Московского университета МВД России имени В. Я. Кикотя, кандидат юридических наук, полковник полиции (г. Москва)
- *Чуманов Александр Сергеевич* – студент 3-го курса юридического факультета Приволжского филиала ФГБОУВО «Российский государственный университет правосудия». Научный руководитель: Головлев Ю. В., доцент кафедры уголовного права Приволжского филиала ФГБОУВО «Российский государственный университет правосудия», кандидат юридических наук, доцент (г. Нижний Новгород)

Секция 2

- *Аксенов Вадим Александрович* – адъюнкт 3-го курса факультета подготовки научно-педагогических и научных кадров Московского университета МВД России имени В. Я. Кикотя. Научный руководитель: Молчанова Т. В., доцент кафедры криминологии Московского университета МВД России имени В. Я. Кикотя, кандидат юридических наук, доцент (г. Москва)
- *Бендас Сергей Родионович* – курсант 2-го «С» курса ИПСОПР Московского университета МВД России имени В. Я. Кикотя. Научный руководитель: Старых С. М., старший преподаватель кафедры уголовного

права ИПСОПР Московского университета МВД России имени В. Я. Кикотя, кандидат юридических наук, полковник полиции (г. Москва)

- *Боровцов Илья Владимирович* – студент 4-го курса юридического факультета Санкт-Петербургского юридического института (филиала) Университета прокуратуры Российской Федерации. Научный руководитель: Гилинский Я. И., профессор Санкт-Петербургского юридического института (филиала) Университета прокуратуры РФ, доктор юридических наук, профессор (г. Санкт-Петербург)
- *Брадул Екатерина Викторовна* – аспирант 1-го курса юридического факультета РГПУ имени А. И. Герцена. Научный руководитель: Милюков С. Ф., профессор кафедры уголовного права Российского государственного педагогического университета имени А. И. Герцена, доктор юридических наук, профессор (г. Санкт-Петербург)
- *Брылева Татьяна Олеговна* – курсант 2-го «Д» курса института-факультета подготовки сотрудников для органов предварительного расследования Московского университета МВД России имени В. Я. Кикотя. Научный руководитель: Ярмонова Е. Н., доцент кафедры административной деятельности Московского университета МВД России имени В. Я. Кикотя, кандидат юридических наук (г. Москва)
- *Войнов Никита Эдуардович* – студент 3-го курса факультета судебных экспертиз и права в строительстве и на транспорте Санкт-Петербургского государственного архитектурно-строительного университета. Научный руководитель: Карнаухова О. Г., доцент кафедры судебных экспертиз СПБГАСУ, кандидат юридических наук, доцент (г. Санкт-Петербург)
- *Воробьева Ольга Дмитриевна* – студент магистратуры юридического факультета Северо-Западного филиала ФГБОУВО «Российский государственный университет правосудия». Научный руководитель: Ялышев С. А., профессор кафедры уголовно-процессуального права Северо-Западного филиала ФГБОУВО «Российский государственный университет правосудия», доктор юридических наук, профессор (г. Санкт-Петербург)
- *Ганюшкина Софья Дмитриевна* – студент 3-го курса Института публичного права и управления Московского государственного юридического университета имени О. Е. Кутафина (МГЮА). Научный руководитель: Саламова С. Я., доцент кафедры криминологии и уголовно-исполнительного права Московского государственного юридического университета имени О. Е. Кутафина (МГЮА), кандидат юридических наук (г. Москва)

- *Гокунь Юлия Сергеевна* – студент 3-го курса юридического факультета ГОУВПО «Донецкий национальный университет». Научный руководитель: Карпенко Л. К., доцент кафедры уголовного права и процесса ГОУВПО «Донецкий национальный университет», кандидат юридических наук, доцент (г. Донецк)
- *Двуличанский Алексей Витальевич* – аспирант 3-го курса кафедры прокурорского надзора и криминологии ФГБОУВО «Саратовская государственная юридическая академия». Научный руководитель: Шляпникова О. В., профессор кафедры прокурорского надзора и криминологии, кандидат юридических наук, доцент (г. Саратов)
- *Журмухамбетова Сания* – студент юридического факультета Казанского (Приволжского) федерального университета. Научный руководитель: Курносова В. В., старший преподаватель кафедры ТиИГиП Юридического факультета КФУ, кандидат юридических наук (г. Казань)
- *Киреева Елизавета Владимировна* – студент 2-го курса Московского университета МВД России имения В. Я. Кикотя ИПСОПР. Научный руководитель: Азаренкова Е. А., старший преподаватель кафедры уголовного права Московского университета МВД России имени В. Я. Кикотя, кандидат юридических наук (г. Москва)
- *Коваленко Мария Андреевна* – аспирант 3-го курса юридического факультета Российского государственного педагогического университета имени А. И. Герцена. Научный руководитель: Милюков С. Ф., профессор кафедры уголовного права Российского государственного педагогического университета имени А. И. Герцена, доктор юридических наук, профессор (г. Санкт-Петербург)
- *Михайлова Анжела Владимировна* – студент магистратуры юридического факультета Северо-Западного филиала ФГБОУВО «Российский государственный университет правосудия». Научный руководитель: Краснова К. А., доцент кафедры уголовного права Северо-Западного филиала ФГБОУВО «Российский государственный университет правосудия», кандидат юридических наук, доцент (г. Санкт-Петербург)
- *Орлова Мария Сергеевна* – слушатель 5-го курса Московского университета МВД России имени В. Я. Кикотя. Научный руководитель: Молчанова Т. В., доцент кафедры криминологии, кандидат юридических наук, доцент, полковник полиции (г. Москва)

- *Панфилов Иван Геннадьевич* – курсант 2-го «С» курса института подготовки сотрудников для органов предварительного расследования Московского университета МВД России имени В. Я. Кикотя. Научный руководитель: Старых С. М., доцент кафедры уголовного права, кандидат юридических наук, полковник полиции (г. Москва)

- *Сарапкин Владимир Александрович* – студент 1-го курса юридического факультета Санкт-Петербургского юридического института (филиала) Университета прокуратуры Российской Федерации. Научный руководитель: Елагина Е. В., доцент кафедры уголовного процесса и криминалистики Санкт-Петербургского юридического института (филиала) Университета прокуратуры Российской Федерации, кандидат юридических наук, доцент (г. Санкт-Петербург)

- *Сидорова Татьяна Сергеевна* – курсант 4-го «У» курса факультета подготовки сотрудников полиции для подразделений по охране общественного порядка, ФГКОУВПО «Московский университет МВД России имени В. Я. Кикотя». Научный руководитель: Вихляев А. А., преподаватель кафедры административной деятельности ОВД факультета подготовки сотрудников полиции для подразделений по охране общественного порядка, ФГКОУВПО «Московский университет МВД России имени В. Я. Кикотя» (г. Москва)

- *Сынков Владимир Владимирович* – студент 4-го курса Санкт-Петербургского юридического института (филиала) Университета прокуратуры Российской Федерации. Научный руководитель: Гилинский Я. И., профессор Санкт-Петербургского юридического института (филиала) Университета прокуратуры РФ, доктор юридических наук, профессор (г. Санкт-Петербург)

- *Сысоева Надежда Николаевна* – курсант 4-го «У» курса факультета подготовки сотрудников полиции для подразделений по охране общественного порядка, ФГКОУВПО «Московский университет МВД России имени В. Я. Кикотя». Научный руководитель: Вихляев А. А., преподаватель кафедры административной деятельности ОВД факультета подготовки сотрудников полиции для подразделений по охране общественного порядка, ФГКОУВПО «Московский университет МВД России имени В. Я. Кикотя» (г. Москва)

- *Саргсян Шаварш* – студент 3-го курса Международно-правового факультета Одинцовского филиала ФГАОУВО «Московский государственный институт международных отношений (университет) Министерства иностранных дел Российской Федерации». Научный руководитель: Решняк

М. Г., доцент кафедры уголовного права, уголовного процесса и криминалистики ОФ МГИМО МИД РФ, кандидат юридических наук, доцент (г. Москва)

- *Цибульская Анжелика Артуровна* – студент магистратуры юридического факультета Северо-Западного филиала ФГБОУВО «Российский государственный университет правосудия». Научный руководитель: Рахманова Е. Н., заведующий кафедрой уголовного права Северо-Западного филиала ФГБОУВО «Российский государственный университет правосудия», доктор юридических наук, доцент (г. Санкт-Петербург)
- *Яблоков Артем Михайлович* – аспирант 2-го года обучения кафедры уголовного права Российского государственного педагогического университета имени А. И. Герцена. Научный руководитель: Дикаев С. У., профессор кафедры уголовного права Северо-Западного филиала ФГБОУВО «Российский государственный университет правосудия», доктор юридических наук, профессор (г. Санкт-Петербург)

Научное издание

КИБЕРПРЕСТУПНОСТЬ: РИСКИ И УГРОЗЫ

материалы Всероссийского студенческого
круглого научно-практического стола с международным участием
(Северо-Западный филиал ФГБОУВО «Российский государственный университет правосудия» (Санкт-Петербург, 11 февраля 2021 г.)

Под ред. д-ра юрид. наук, доцента Е. Н. Рахмановой

Сост. и ред.: К. А. Краснова, Е. В. Топильская, Е. А. Васик

ЦНИТ «Астерион»
Заказ: № 061. Подписано в печать: 21.04.2021. Бумага офсетная.
Формат: 60x84 1/16. Объем: 30 п. л. Тираж: 200 экз.
Санкт-Петербург, 191015, а/я 83,
тел.: (812) 685-73-00, 663-53-92, тел. 970-35-70
e-mail: asterion@asterion.ru http://www.asterion.ru
https://vk.com/asterion_izdatelstvo